



AFRL-RI-RS-TR-2014-022

CLUSTER STATE QUANTUM COMPUTATION

FEBRUARY 2014

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

**AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (<http://www.dtic.mil>).

AFRL-RI-RS-TR-2014-022 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /

STEVEN T. JOHNS
Chief, Trusted Systems Branch

/ S /

MARK LINDERMAN
Technical Advisor, Computing &
Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) FEBRUARY 2014		2. REPORT TYPE FINAL TECHNICAL REPORT		3. DATES COVERED (From - To) NOV 2010 – SEP 2013	
4. TITLE AND SUBTITLE CLUSTER STATE QUANTUM COMPUTATION				5a. CONTRACT NUMBER IN-HOUSE	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER 62788F	
6. AUTHOR(S) Paul Alsing, Michael Fanto, and Gordon Lott				5d. PROJECT NUMBER T2QC	
				5e. TASK NUMBER IN	
				5f. WORK UNIT NUMBER HO	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/Information Directorate Rome Research Site/RITA 525 Brooks Road Rome NY 13441-4505				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/Information Directorate Rome Research Site/RITA 525 Brooks Road Rome NY 13441-4505				10. SPONSOR/MONITOR'S ACRONYM(S) AFRL/RI	
				11. SPONSORING/MONITORING AGENCY REPORT NUMBER AFRL-RI-RS-TR-2014-022	
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited. PA# 88ABW-2014-0342 Date Cleared: 4 Feb 14					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This is the final report for the AFRL/RI in-house project Cluster State Quantum Computation. Under this project investigations were conducted which included: (i) the development and characterization of a new multipli-entangled photon source that increased the usable number of photon pairs by a factor of six over conventional entangled photon sources; (ii) design of multi-layer superconducting number-resolving photon detector, (iii) a theoretical and experimental investigation into the requirements of imperfect (non-unit fidelity) two-qubit linear optical photonic gates; (iv) a theoretical investigation of entanglement and nonlocality addressing the issue of why nature does not take advantage of the algebraically allowed maximum correlations amongst collections of qubits, and (v) a theoretical investigation into the a 2.25X more efficient means to generate linear cluster states. This latter investigation led to a patent for probabilistic cluster state generator, also discussed in this report.					
15. SUBJECT TERMS Quantum information processing, quantum computing, quantum entanglement					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 81	19a. NAME OF RESPONSIBLE PERSON Paul M. Alsing
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) N/A

TABLE OF CONTENTS

LIST OF FIGURES	ii
LIST OF TABLES	iii
1.0 SUMMARY	1
2.0 INTRODUCTION	1
3.0 METHODS, ASSUMPTIONS AND PROCEDURES	4
3.1 Multipli-entangled photons from a spontaneous parametric down-conversion source.....	4
3.2 A multi-layer three dimensional superconducting nanowire photon detector	9
3.3 Theory/experimental requirements of imperfect two-qubit linear optical photonic gates	11
3.4 Nonlocality, entanglement witnesses and supra-correlations	13
3.5 Efficient cluster state generation (theory)	20
4.0 RESULTS AND DISCUSSION	26
4.1 Multipli-entangled photons from a spontaneous parametric down-conversion source.....	26
4.2 A path towards experimental generation of a linear cluster state	29
4.3 A multi-layer three dimensional superconducting nanowire photon detector	34
4.4 Laboratory upgrade and ongoing research in integrated waveguide quantum circuits.....	35
4.5 Probabilistic cluster state generator patent.....	36
4.6 Theory/experimental requirements of imperfect two-qubit linear optical photonic gates	44
4.7 Nonlocality, entanglement witnesses and supra-correlations	48
4.8 Efficient cluster state generator (theory).....	54
5.0 CONCLUSIONS.....	64
6.0 REFERENCES	67
7.0 LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS.....	73

LIST OF FIGURES

Figure 1: Kwiat's type I pair	5
Figure 2: Standard type II down conversion	6
Figure 3: Imaging of the down-converted light for three different configurations	6
Figure 4: Type II crystal assembly as described by [Bittion01]	7
Figure 5: Type II custom assembly showing alternating layers of β -BBO and calcite.....	7
Figure 6: Cascaded and multi-pass crystal configurations for the generation of cluster states [Lu07]	8
Figure 7: Type-II SPDC Schioedtei source.....	9
Figure 8: A single superconducting nanowire "pixel" bridge.....	10
Figure 9: Plan view of final device with all three layers aligned on top of each other	11
Figure 10: CHSH inequality derived as a violation of the classical quadrilateral inequality	15
Figure 11: PR Box probability achieving the algebraic maximum $S_M=4$ of the CHSH inequality	18
Figure 12: A general measurement-assisted transformation using a linear optical interferometer	22
Figure 13: State transformation & detection of a photon in either one of two modes of a dual-rail pair ...	23
Figure 14: Experimental testbed to analyze the Schioedtei source.....	26
Figure 15: False color CCD images of custom crystal assembly (1 sec exposure).	27
Figure 16: Alignment image of the Schioedtei crystal stack	27
Figure 17: Experimental setup for 4-qubit cluster state generation utilizing Schioedtei	28
Figure 18: Experimental construction of a 4-qubit box cluster state utilizing Schioedtei	29
Figure 19: Entangled photon collection and measurement system.....	30
Figure 20: Density matrix of both measured pairs of photons.....	31
Figure 21: Controlled Phase gate system.....	32
Figure 22: Free space polarization control and measurement system.....	33
Figure 23: Professionally assembled polarization controller and measurement systems	34
Figure 24: A plain view of the three layers in the multilayer design.....	34
Figure 25: A toy model of a multi-layer SNSPD.....	35
Figure 26: Sequential entangler	37
Figure 27: Symmetric sequential entangler	38
Figure 28: Two dimensional cluster state generator	39
Figure 29: Probabilistic cluster state generator	40
Figure 30: Rotation matrix for modes $N-1$ and N	45
Figure 31: Improved success rates for compromised δ	46
Figure 32: Beamsplitter transmissivity	47

Figure 33: General multiport device schematic.	47
Figure 34: PR Box shared between Alice and Bob.....	48
Figure 35: Numerical simulations for $m=\{2,3,4,\dots,12\}$ measurement vectors	52
Figure 36: Numerical results for generation of C_4 cluster state from a pair of two Bell states.....	55
Figure 37: Success probability for C_6 (left) and C_8 (right) CS generation from three Bell states.....	56
Figure 38: Success probability for C_6 (left) and C_8 (right) CS generation from product states.....	57
Figure 39: Fusing a single qubit to a C_n cluster	60
Figure 40: Fusion of a single qubit to the <i>end</i> of an n -qubit linear cluster state	61
Figure 41: Fusion of a single qubit to the <i>middle</i> of an n -qubit linear cluster state	63

LIST OF TABLES

Table 1: Quantum tomography measurements, waveplate positions and measured concurrence	31
Table 2: Results of success probability of cluster state generation.....	58

1.0 SUMMARY

Experimental, theoretical and numerical investigations of quantum computation using photon-based qubits were conducted to explore the Cluster State (or one-way) Quantum Computing paradigm. This report describes research on a unique type II SPDC source (Schioedtei) design that can generate up to six pairs of entangled photons per pass through the type II crystal assembly. This source is currently being used as the entangled photon source to create photon-based qubit cluster states. Under this project we developed a new detector design architecture that turns the single photon detector into a number-resolving detector by means of a novel three dimensional architecture that utilizes spatial multiplexing. We have studied the CNOT gate, as an archetypical quantum linear optical gate, and found several interesting features in the both the ideal and the realistic case of implementation with imperfect (non-unit) fidelity. We conducted a theoretical investigation of the limitations of quantum correlations imposed the physically imposed constraint of no-signaling (i.e. no faster than light communication). Finally, we developed a more efficient means to generate linear cluster states from which we designed a probabilistic cluster state generator (patent submitted).

2.0 INTRODUCTION

Under this AFRL/RI in-house project Cluster State Quantum Computation we continued research and development of a novel multi-qubit entangled photon source, begun under the AFRL/RI in-house project “Quantum Information Science (QIS),” (AFRL-RI-RS-TR-2012-073), and conducted investigations into the measurement based cluster state quantum computation paradigm utilizing photon-based qubits. These investigations included: (i) the development and characterization of a new multipli-entangled photon source that increased the usable number of photon pairs by a factor of six over conventional entangled photon sources; (ii) design of multi-layer superconducting number-resolving photon detector, (iii) a theoretical and experimental investigation into the requirements of imperfect (non-unit fidelity) two-qubit linear optical photonic gates; (iv) a theoretical investigation of entanglement and nonlocality addressing the issue of why nature does not take advantage of the algebraically allowed maximum correlations amongst collections of qubits, and (v) a theoretical investigation into the a 2.25X more efficient means to generate linear cluster states. This latter investigation led to a patent for probabilistic cluster state generator, also discussed in this report. In addition, this report discusses upgrades to our in-house AFRL/RI Quantum Computing Laboratory under the current project and our thrust to transition our development of quantum gates/circuits in bulk optics to an on chip integrated waveguide implementation.

Cluster State Quantum Computation Background

In the standard quantum circuit model (QCM) paradigm, quantum computations are executed by successive unitary operations acting upon an initial quantum state composed of many qubits. These unitary operators create entanglement amongst the qubits through quantum interference. Entanglement is uniquely non-classical property of quantum mechanical systems in which the correlations between sub-systems can be stronger than that allowed by classical (conventional) computing systems. Recently a new alternative paradigm for quantum computation has emerged called one-way quantum computation (OWQC) [Ruassendorf01]. In the one-way quantum computer, information is processed by sequences of single-qubit measurements. These measurements are performed on a universal resource state—the 2D-cluster state—which does not depend on the algorithm to be implemented. The new approach to quantum computation goes

by the collective name measurement-based quantum computation (MBQC) [Briegel09]. The appeal of MQC is that deterministic quantum computation is possible based on (i) the preparation of an initial entangled cluster state followed by (ii) a temporally ordered pattern of single qubit measurements and feed-forward operations which depend on the outcome of the previously measured qubits [Raussendorf01]. Our interests in OWQC is in the utilization of photon-based cluster states as gates and circuits for quantum computation (see [Vallone08], and references therein). It has been claimed that the use of cluster states can substantially reduce the resource overhead in the standard QCM to photon-based quantum computation.

In the OWQC approach a quantum computation proceeds as follows: (i) a classical input is provided which specifies the data and the program; (ii) a 2D-cluster state of sufficiently large size is prepared. The cluster state serves as the resource for the computation; (iii) a sequence of adaptive one-qubit measurements is implemented on certain qubits in the cluster. In each step of the computation the measurement bases depend on the specific program under execution and on the outcomes of previous measurements. A simple classical computer is used to compute which measurement directions have to be chosen in every step; (iv) after the measurements the state of the system has the product form $|\xi^\alpha\rangle|\psi_{out}^\alpha\rangle$, where α indexes the collection of measurement outcomes of the different branches of the computation. The states $|\psi_{out}^\alpha\rangle$ in all branches are equal to the desired output state up to a local (Pauli) operation. The measured qubits are in a product state $|\xi^\alpha\rangle$ which also depends on the measurement outcomes. The OWQC is computationally universal, i.e. even though the results of the measurements in every step of the computation are random, any quantum computation can deterministically be realized. Notice that the temporal ordering of the measurements plays an important role and has been formalized as a feed-forward procedure [Raussendorf01].

In realistic physical systems decoherence tends to make quantum systems behave more classically. One could therefore expect that decoherence would threaten any computational advantage possessed by a quantum computer. However, the effects of decoherence can be counteracted by quantum error correction [Shor96]. In fact, arbitrarily large quantum computations can be performed with arbitrary accuracy provided the error level of the elementary components of the quantum computer is below a certain threshold. This important result is called the threshold theorem of quantum computation [Aliferis06].

Fault-tolerant schemes for OWQC using photons have recently been developed [Dawson06, Varnava06]. The dominant sources of error in this setting are photon loss and gate inaccuracies. The constraint of short-range interaction and arrangement of qubits in a 2D lattice—a characteristic feature of the initial one-way quantum computer—is not relevant for photons. In [Dawson06] both photon loss and gate inaccuracies were taken into account yielding a trade-off curve between the two respective thresholds. Fault-tolerant optical computation is possible for a gate error rate of 10^{-4} and photon loss rate of 3×10^{-3} . In [Varnava06] the stability against the main error source of photon loss was discussed. With non-unit efficiencies η_S and η_D of photon creation and detection being the only imperfections, the very high threshold of $\eta_S \eta_D > 2/3$ was established. Further, encoding a collection of physical qubits within the 2D cluster state offers a means of topological error protection for the logical qubit. Topologically protected quantum gates are performed by measuring some regions of qubits in the Z-basis, which effectively

removes the qubits from the state. The remaining cluster, whose qubits are measured in the X- and $X \pm Y$ -basis, thereby attains a non-trivial topology in which fault-tolerant quantum gates can be encoded. A topological method of fault-tolerance for OWQC can then be achieved [Raussendorf07].

Experimental Research:

Photons are particularly desirable for quantum information processing tasks since they are relatively free from environmental decoherence. Hence, they are also essential for any long distance conveyance of quantum information, and do not require cryogenic cooling. Entangled photon sources with the highest mode quality are based on spontaneous parametric down conversion (SPDC). This is a process where laser pump photons are converted into ‘signal’ and ‘idler’ entangled pairs in nonlinear (NL) crystals. SPDC in nonlinear crystals has provided the optical sources for groundbreaking foundational and applications work in quantum optics (QO) for the last two decades [O’Brien07].

SPDC is an inherently inefficient process, and work based on it is generally limited by the net signal level or the number of photons that can be entangled in given applications. Photon yield is related to laser power, which cannot be increased beyond the level where higher order NL contributions (multi-photon events) yield errors in quantum processing applications. This point has now been reached in applications that require independent sources of entangled qubits. The work begun under the in-house Quantum Information Science project focused on (i) developing a 6-qubit capable photon-based quantum information testbed and (ii) initial development of new sources of entangled photons that greatly increase process efficiency, without increasing laser power, in a regime where high detection quantum efficiency is available - a highly desirable goal not previously accomplished in the scientific community to date. This latter direction of research was continued and expanded upon in the current in-house project Cluster State Quantum Computing.

Number resolving photon counting at the single photon level, i.e. distinguishing 1, 2 or 3 photons is an important experimental ability. While experiments can be performed without number resolving detectors such as the APD we are currently using, a significant number of interesting experiments requires the number resolving ability. Therefore we considered a known single photon detector (click or no-click) and have developed a new detector design architecture that turns the single photon detector into a number-resolving detector. This is done through spatial multiplexing. The architecture we have developed allows for higher density of detection elements and larger number of detector elements than the current state of the art. This leads to faster repetition times and most importantly superior number resolution.

Theory/Numerical Research:

The creation of single photons is most often performed by non-linear processes such as SPDC, however to create cluster states from these resource photons requires linear optics, such as the CNOT or CZ gates. Numerous implementation methods have been suggested for these gates in theory, however in practice any implementation will be imperfect. Therefore it is important to be able to characterize and optimize imperfect, i.e. fidelity less than 1, linear optical gates and state transformations. We have studied the CNOT gate, as an archetypical linear optical gate and found several interesting features in the both the ideal case and the realistic case of imperfect fidelity. In particular we find that the success rate can be increased as the fidelity decreases.

This trade off in fidelity for success opens several interesting possibilities in the field of linear optics. We also found that the CNOT gate has a high degree of symmetry that simplifies its physical implementation in both cases and proposed a practical experiment to test our theories. Such studies can and have been carried over to other gates and state transformation with relative ease.

The ultimate goal of MBQC is to execute quantum algorithm with speedup over their corresponding counterpart classical algorithms. Under this project we began an investigation of Grover's search algorithm (on an unsorted list of elements) in the MBQC paradigm and its comparison/contrast with the usual QCM approach. Grover's search algorithm (GSA) serves as an important prototypical benchmark for many numerical simulation efforts of quantum algorithms [Grover97, Walther05]. Our preliminary results (which are currently being written up for journal submission) indicate that the MBQC implementation of Grover's algorithm is faster than even Grover's quantum algorithm (with its quadratic speedup over a brute force search).

In brief, Grover's oracle based unstructured search algorithm is often stated as "given a phone number in a directory, find the associated name." More formally, the problem can be stated as "given as input a unitary black box U_f for computing an unknown function $f: \{0,1\}^n \rightarrow \{0,1\}$ find $x=x_0$ an element of $\{0,1\}^n$ such that $f(x_0)=1$, (and zero otherwise)." The crucial role of the externally supplied oracle U_f (whose inner workings are unknown to the user) is to change the sign of the solution $|x_0\rangle$, while leaving all other states unaltered. Thus, U_f depends on the desired solution x_0 . Under the previous in-house QIS project, we developed/simulated an amplitude amplification algorithm in which the user encodes the directory (e.g. names and telephone numbers) into an entangled database state, which at a later time can be queried on one supplied component entry (e.g. a given phone number t_0) to find the other associated unknown component (e.g. name x_0). For $N=2^n$ names $|x\rangle$ with N associated phone numbers $|t\rangle$, performing amplitude amplification on a subspace of size N of the total space of size N^2 produces the desired state $|x_0\rangle|t_0\rangle$ in \sqrt{N} steps.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1. Multipli-entangled photons from a spontaneous parametric down-conversion source

Photon based quantum computation, with single or entangled photons, is a heavily researched area. This is in part due to many desirable properties of photons such as (i) room temperature operation, (ii) immunity from the environment and (iii) superior mode quality. Spontaneous parametric down conversion has proven to be the most reliable method of generating entangled photon pairs. Type I sources spontaneously convert one linearly polarized parent photon into two daughters, each having an orthogonal polarization to the parent. The spontaneous nature of parametric down conversion produces a ring pattern where each diametric photon pair shares the same parent photon. Because the type I process produces two photons of the same polarization which are path entangled. That is, detecting a photon (signal) in path A implies that its sister (idler) can be found in the diametrically opposite spot [Dragoman01]. This implies that in the polarization basis a mixed state $|H\rangle_1|H\rangle_2$ or $|V\rangle_1|V\rangle_2$ will be produced. Many experiments that require photon pairs, but not entangled pairs, use the output of a type I crystal as input to a more sophisticated experiment. Type I crystals are inherently birefringent, but the walk-off associated

with these crystals is mitigated by the fact that the down converted photons are the same polarization; the delays that the signal and idler photons experience are the same. Type I sources have been used for many years in harmonic generation (SHG, THG) systems as frequency converters.

Kwiat first described a feasible source for SPDC-generated entangled pairs using type I β -BBO [Kwiat99] (beta-Barium borate, BaB_2O_4). This consisted of a stacked pair of type I crystals rotated 90° relative to each other (Figure 1). This allows for the generation of two orthogonally polarized cones that overlap in space. Each crystal can only be excited by a certain linear polarization. The stack must be pumped by a beam made up of components that excite each crystal equally. That is, if the stack consists of an optic axis that is vertical in the first crystal, and horizontal in the second, the pump beam polarization must be oriented at 45° . The resulting superposition state is $|H\rangle_1|H\rangle_2 \pm e^{i\theta} |V\rangle_1|V\rangle_2$. It is important to note that there is a temporal delay associated with the down converted states due to the crystal's birefringence. Compensation depends on the wave packet of the pump photon.

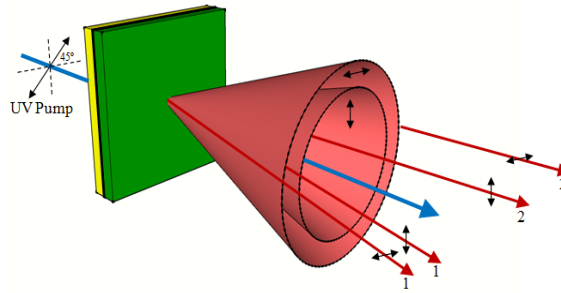


Figure 1. Kwiat's type I pair. Each crystal will spontaneously down convert a linearly polarized photon pair orthogonal to its pump photon. When specifically oriented, these down converted rings can overlap and create a polarization entangled pair.

Type II sources [Kwiat95] down convert a linearly polarized parent photon into two orthogonally polarized daughters making them particularly interesting because the crystal is birefringent. One daughter photon will walk off faster than the other and lead to a noticeable spatial separation, and thus two intersecting cones (Figure 2). The walk off of type II crystals limits the length of the crystal because the extraordinary index of refraction will quickly bend light out of the crystal. Indistinguishable photons are produced in the intersections of the two cones. These two points form a superposition state of polarization ($|H\rangle_1|V\rangle_2 \pm e^{i\theta} |V\rangle_1|H\rangle_2$) and have been exhaustively studied and used as inputs to more complex photonic systems. Figure 3 shows the evolution of the rings of entangled photons produced from SPDC crystals under type I and II phase matching conditions.

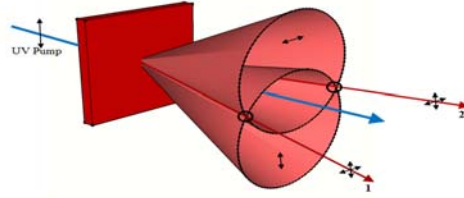


Figure 2. Standard type II down conversion. A linear pump beam spontaneously down converts to two photons, one of which has the same polarization as the pump. The other is orthogonal. The familiar double ring pattern is a product of the crystal's birefringence.

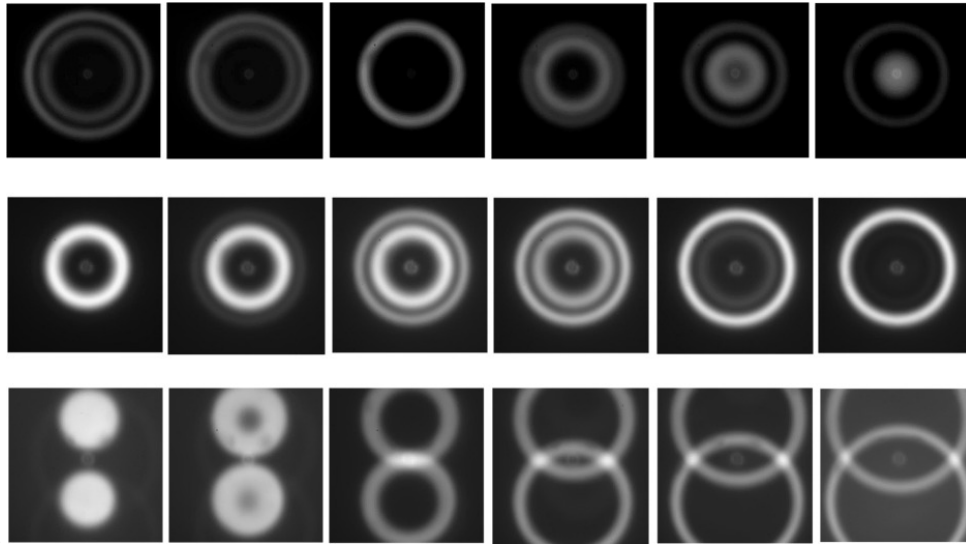


Figure 3: Imaging of the down-converted light for three different configurations. First row: type-I SPDC as a function of the tilt of one crystal. Second row: type-I SPDC rings of different diameters as a function of the polarization of the pump beam (horizontal on the left and vertical on the right). Third row: type-II SPDC rings as a function of the tilt of the crystal. All cases involve the CW pump laser beam.

In a similar fashion to Kwiat's type I stack, Bitton et al. [Bitton01] described a type II stack comprised of two crystals rotated 180° relative to each other (Figure 4). This allows the linear pump scheme to remain unchanged and yields one set of rings from either crystal. The set of rings entirely overlap each other and thus can yield an entangled photon pair of the same state as standard type II. Addressing the compensation is a necessary requirement with any birefringent crystals. A standard type II stacked configuration allows for greater pair production and more useable detection area. In this source as well as a type I stack, the fundamental size of the collection apertures become the limiting factor in the number of entangled pairs that can be collected.

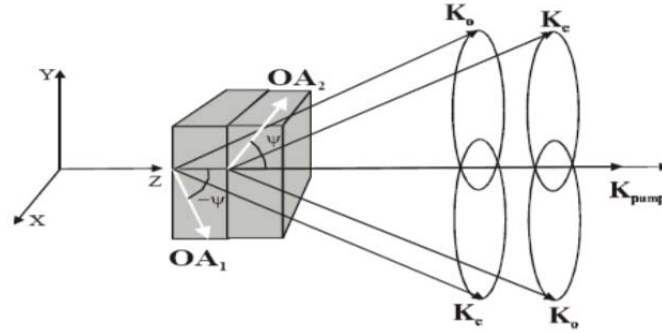


Figure 4. Type II crystal assembly as described by [Bittion01]. The second crystal is rotated 180° relative to the first, resulting in two overlapping sets of cones with orthogonal polarization.

U'ren et al. [U'ren06] described a type II crystal assembly (Figure 5a) that is designed for group velocity matching (GVM) of the pump and signal/idler wave packets, thereby removing any spectral distinguishability of the down converted photons. The assembly consists of a successive stack of nonlinear crystals (β -BBO, BiBO (Bismuth Borate, BiB_3O_6)) separated by a thin layer of compensating crystal (calcite (CaCO_3), α -BBO). This aims to slowly compensate different components (pump and down converted wave packets) such that by the end of the stack there is no spectral walk off. The need to spectrally filter post down conversion is mitigated by the symmetry of their joint spectral function (Figure 5b). Removing this requirement typically increases the useable count rate and overall efficiency.

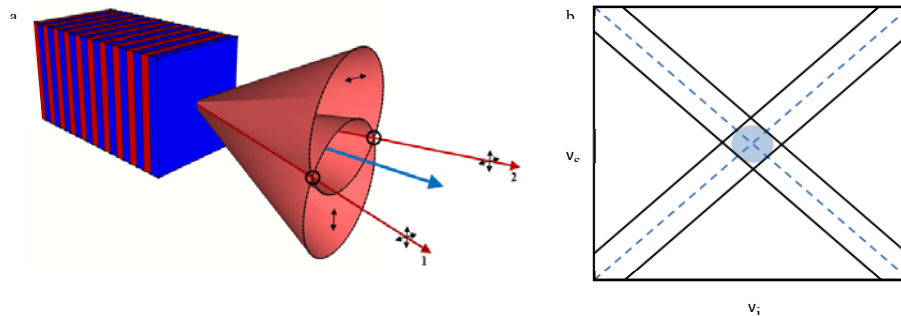


Figure 5. (a) Type II custom assembly showing alternating layers of β -BBO (red) and calcite (blue). (b) Joint spectral function of down converted wavepacket. This implies a maximally separable state.

Type I and II crystals are still governed by their spontaneous nature, and this becomes problematic when large numbers of entangled photons are required. In a typical configuration for the generation of greater than four photons a cascaded apparatus is used. For this setup either multiple crystals are used in succession, or multiple passes through a single crystal (Figure 6). This implies an overall increase in footprint size. Hyper-entanglement has been considered to mitigate the spontaneous nature of down conversion by adding entanglement various degrees of freedom, not just polarization [Ceccarelli09]. While this is effective it adds to the expense of larger physical hardware requirements and more complicated analysis processes.

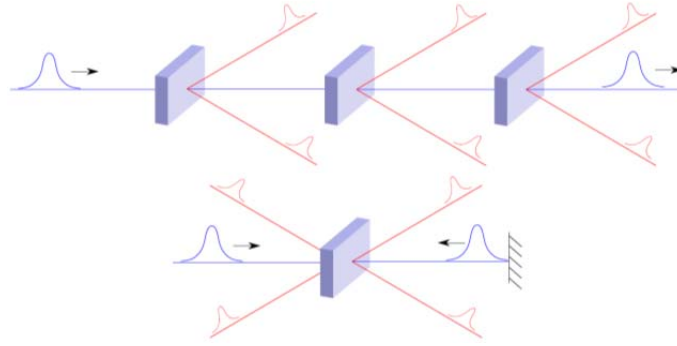


Figure 6. Cascaded and multi-pass crystal configurations for the generation of cluster states [Lu07].

In recent years there has been a paradigm shift in quantum computation with the need to migrate toward schemes that require only single qubit measurements. One-way quantum computation (cluster state) has facilitated this shift. Cluster state computation allows a predetermined sequence of single qubit measurements to determine the algorithm being evaluated [Walther05]. This protocol requires a highly entangled cluster state [Raussendorf01] generated from a resource of qubits. Such a cluster state can be constructed by preparing each of the qubits into a state, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and applying controlled-phase gates to link the required qubits. Computation proceeds with a sequence of single qubit measurements whose results will classically feedforward to control the basis required for future measurements [Nielson05]. Cluster state computation allows for a practical resource reduction in qubits and hardware compared to other quantum computing methods. That being said, the fundamental requirement for larger numbers of qubits still exists. The source we have developed produces larger qubits numbers than that of a typical type II SPDC source.

SPDC custom crystal assembly

Our custom two-crystal assembly (designated as “Schioedtei” henceforth) design consists of a pair of type II non-collinear phase-matched SPDC crystals cut for degenerate down-conversion whose optic axes are rotated orthogonal with respect to one another. The pair of crystals is optically contacted with one another and a dual band (405/810 nm) anti-reflection coating applied to the two exterior faces of the assembly. Any type II material can be used to create an equivalent device. Our particular version that will be discussed here was constructed from two 8x8x2 mm type II beta-Barium borate (β -BBO, BaB_2O_4) crystals phase matched (at angles of $\theta = 41.9^\circ$, $\phi = 30^\circ$) for 810 nm spontaneous parametric down-conversion.

Exciting Schioedtei with an incident 45° polarized pump beam produces one pair of rings from each of the type II crystals. Each pair of rings is orthogonal to the other resulting in 12 intersection points (or simply “points”) where indistinguishable photons are produced. Referring to Figure 7, the indicated points marked 5, 6 (Bell pair #1 from crystal #1) and 7, 8 (Bell pair #2 from crystal #2) are the typical Bell states, $|\psi\rangle_{5,6(7,8)} = \frac{1}{\sqrt{2}}(|HV\rangle_{5,6(7,8)} \pm e^{i\phi}|VH\rangle_{5,6(7,8)})$. The

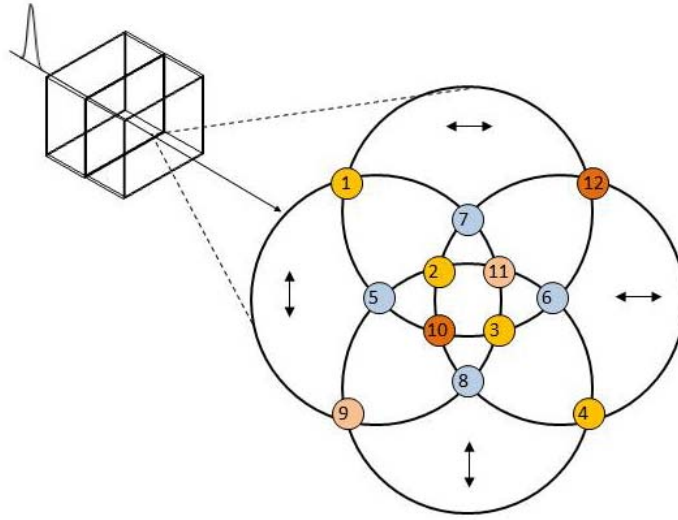


Figure 7. Type-II SPDC Schioedtei source. See text for discussion of the intersection points of the overlapping rings.

points indicated by 1, 2, 3, 4 are the product of two bell states, $|\psi\rangle_{1,2,3,4} = \frac{1}{2} (|HV\rangle_{1,4} \pm e^{-i\varphi} |VH\rangle_{1,4}) (|HV\rangle_{2,3} \pm e^{-i\varphi} |VH\rangle_{2,3})$, produced from photons from both crystal 1 and 2 concurrently. Points 9, 11 and 10, 12 are $|VV\rangle_{9,11}$ and $|HH\rangle_{10,12}$ states produced from photons from crystal 1 and 2 concurrently. Further analysis and experimental results of Schioedtei are covered in section 4.1.

3.2 A multi-layer three dimensional superconducting nanowire photon detector

Construction of photon-counting devices with high counting efficiency, high number resolution and short reset times, is highly desirable for a wide array of applications, such as quantum key distribution [Xu08], quantum communication [O’Brein09], quantum computing [Knill01], [Uskov10], [Knill02] among others [Hadfield09], [Smith11]. Here we describe and perform some simple analysis of a proposed detector design that uses multiple short sections of superconducting nanowires to construct a new superconducting nanowire single photon detector (SNSPD). We refer to these short sections of nanowire as pixels and arrange them in a two dimensional grid in analogy with a standard CCD camera. We will discuss the potential advantages in such a system and the difficulties of the design.

When an incident photon strikes a Niobium nitride (NbN) nanowire, or other superconducting material such as NbTiN or a- W_xSi_{1-x} developed recently at NIST, it creates a resistive hot spot [Nam11]. This hot spot causes the current in the superconductor to deflect around the spot, thus increasing the current density in the wire. This increased current density leads to an increase in the temperature of a small section of the wire. If the nanowire is held just below the critical current for superconduction, then the increase in heat will break the superconducting condition and the resistance of the wire will spike upward for a short time. This resistance spike creates a measurable current in the external resistance load and a photon is counted.

Present superconducting nanowire systems, such as NbN, have reasonably good counting efficiency [Dauler10], [Marsili11], by which we mean the probability of an incident photon being detected is over 25%. However, a significant problem exists with the number resolution, relaxation time and fill factors [Gurevich87], [Dauler10], [Marsili11]. A detector consisting of a single wire can be made to cover a significant detection area by creating a meander. Usually this means folding the nanowire back and forth across the desired area of approximately $10\mu\text{m} \times 10\mu\text{m}$ [Dauler10], [Marsili11]. This however is not a number resolving detector. All that the detector can feel is the loss of the superconducting condition somewhere in the nanowire. Should two photons strike the wire simultaneously in two different locations the current drop is very similar. One suggested solution to this lack of number resolving capability is to increase the number of wires in the meander. This has been done experimentally by Dauler et al.[Dauler10]. While this approach improves on the single wire meander it still consists of long wires each of which occupies a significant portion of the active detection area (i.e. each nanowire in a 4-nanowire meander takes approximately 25% of the active area). In order to have a high probability of correctly detecting n number of photons one would need significantly more than n wires.

We proposed a detector design using short sections of wire, which we will refer to as pixels, that are arranged in a 2D grid to create the detection area. Such a design would use a large number of pixels thus giving high number resolution and the small size of the pixels gives short relaxation times. We call this configuration a multi-layer superconducting number-resolving photon detector. A significant problem with creating a two dimensional array of nanowire pixels is the question of how to attach the leads to each pixel, as the leads are of a similar size as the pixels themselves. One could simply move the pixels farther and farther apart to fit in all the necessary connections but this is impractical as the space between pixels does not detect photons and the device's overall efficiency would decrease below useful levels. Ideally the pixels will be packed as closely as possible, while still avoiding cross talk. This will maximize the so called fill factor, the ratio of the photon sensitive area to the non-sensitive area within the “active” area of the detector. We therefore propose moving away from the two dimensional approaches used to date

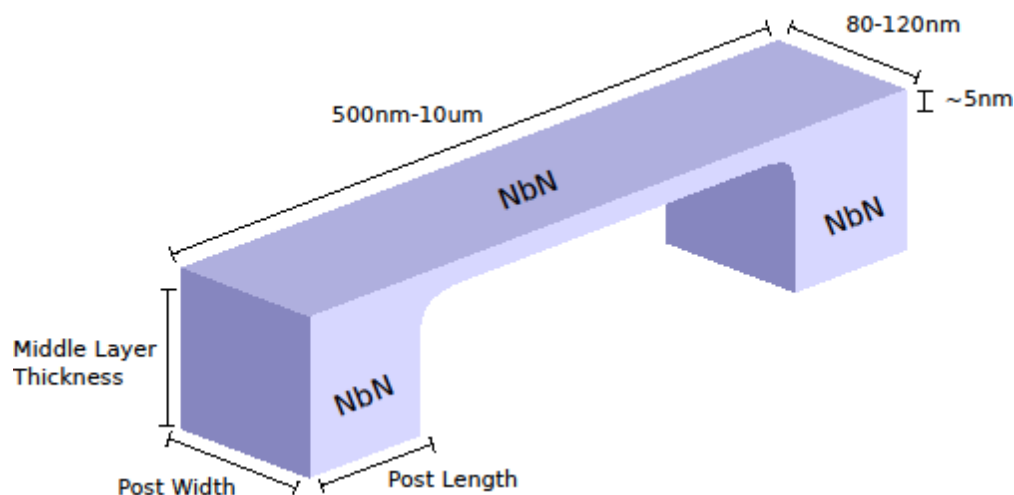


Figure 8. A single superconducting nanowire “pixel” bridge.

and instead suggest a multilayer, three dimensional architecture. We therefore proposed moving away from the two dimensional approaches used to date and instead suggest a multi-layer, three dimensional architecture. In this scheme the non-superconducting leads are allowed to pass under the active detector pixels. To create this effect we shape the pixels like small bridges as seen in Figure 8. This shape was chosen because of its relatively simple design and in order to maximize the fill factor.

This creates a 3 layer design, with the bottom layer containing the leads, an insulating middle layer, and the active detection layer on top. We now show a bird's eye view (plan view) of the final device with all three layers aligned on top of each other, Figure 9. The black arrows show the movement of the current throughout the device.

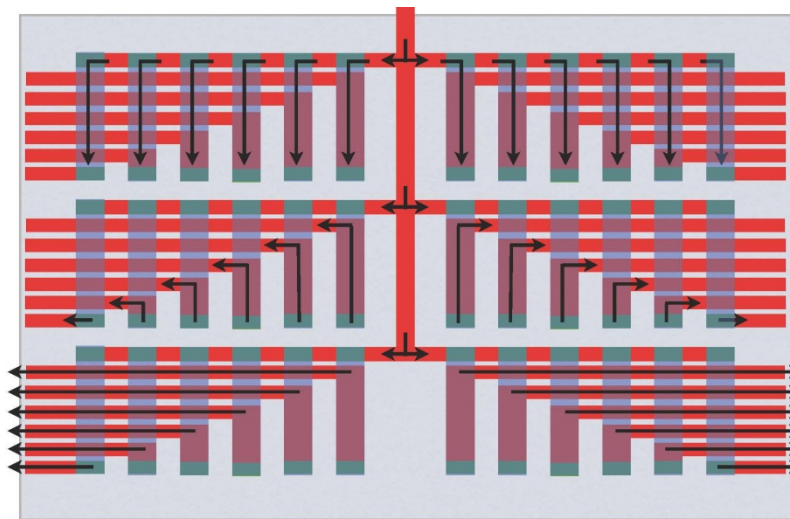


Figure 9. Plan view of final device with all three layers aligned on top of each other.

The current enters the detector in the bottom layer (red) through the shared input lead (center of figure). Current then moves up through the middle layer connections, called “posts” (green), to the top/detection layer. Once in the top layer it moves along the surface of the bridge (purple). This is the area in which an incident photon will form a resistance blockage. The current then moves back down to the bottom layer and is channeled out of the device by the output leads (red). Note that the leads (red) pass under the pixel bridges, between the posts and that the input/output leads are all on the same layer. The external detection electronics would then be similar industry standards. As a final aside each pixel can be wired as a completely independent circuit, but the number of leads will increase and counting simultaneous events between elements can become difficult.

3.3 Theory/experimental requirements of imperfect two-qubit linear optical photonic gates

Knill, Laflamme, and Milburn (KLM) significantly advanced the prospect of single-photon quantum computing in their seminal paper [Knill01], in which they overcame the need for nonlinear interactions by using the inherent nonlinearity of photon measurements. In this scheme, the computational system is combined with ancillary modes, and the gate operation is performed on the enlarged state space. The ancilla modes are measured with photon-number-

resolving detectors, such as those described above leaving the computational modes undisturbed and in the desired output state provided the measurement is successful. In our previous work [Uskov10, Uskov09, Smith11], we have shown that a combination of analytical and numerical techniques may be used to design optimal linear optical transformations implementing two- and three-qubit entangling gates. Here we show results for non-ideal gates and suggest an experiment to test them.

The probabilistic nature of quantum measurement implies a trade-off between the success rate of the operation (the probability of obtaining the desired measurement outcome for the ancillary modes) and the fidelity (the overlap between the actual and desired states of the computational system when the ancilla measurement is successful). Previously, solutions were obtained that have the maximum possible ancilla measurement success probability given the constraint of perfect fidelity for a specified transformation [Uskov10, Uskov09]. In practical implementations, however, the goal of perfect fidelity may not always be desirable or even attainable. We have therefore generalized our previous techniques to the case of imperfect fidelity, and investigated the above-mentioned trade-off between the fidelity and success of the linear optical transformations. It was found that for sufficiently small deviations from perfect fidelity, a single optimization parameter determines the relationship between fidelity and optimal success rate [Smith11].

The input state to the experiment $|\Psi^{\text{comp}}\rangle_{\text{X}}|\Psi^{\text{ancilla}}\rangle$ is a product of the computational state containing M_c photons in N_c modes, and an ancilla state containing M_a photons in N_a modes. The N_c computational modes are those on which the actual gate is intended to act. Assuming dual-rail encoding, each qubit is represented by one and only one photon in two computational modes, so we have $M_c = N_c = 2$. The ancilla state may in general be separable, entangled, or an ebit state carrying spatially distributed entanglement [Wilde09], though here we propose using only a product state of single-photon and zero-photon ancillas, which are relatively simple to produce in an experimental setting.

The linear optical device transforms the creation operator $a_i^{(in)\dagger}$ associated with each input mode i to a sum of creation operators $\sum_j U_{i,j} a_j^{(out)\dagger}$. Here U , which contains all physical properties of the device, is an $N \times N$ matrix, where $N = N_c + N_a$ is the total number of modes. The total input state may be written as a superposition of Fock states $|\Psi\rangle = |n_1, n_2, \dots, n_N\rangle$, where n_i is the occupation number of the i -th input mode, and $\sum n_i = M_c + M_a = M$ is the total number of photons. The input state is transformed as

$$|\Psi_{out}\rangle = \Omega |\Psi_{out}\rangle = \prod_{i=1}^N \frac{1}{\sqrt{n_i!}} \left(\sum_{j=i}^N U_{i,j} a_j^{(out)\dagger} \right)^{n_i}. \quad (1)$$

We note that Ω is a multivariate polynomial of degree M in the elements $U_{i,j}$. Once the transformation is complete, a measurement is applied to the N_a ancillary modes. In the case of a number-resolving photon-counting measurement, $\langle \Psi_{measured} | = \langle K_{N_c+1}, K_{N_c+2}, \dots, K_N |$, where K_i is the number of photons measured in the i -th mode of the ancilla. The resulting transformation of the computational state is a contraction quantum map $|\Psi_{in}^{comp}\rangle = A |\Psi_{in}^{comp}\rangle / \|A |\Psi_{in}^{comp}\rangle\|$ [Kraus83], where $A = A(U)$ is defined by,

$$A|\Psi_{in}^{comp}\rangle = \langle K_{N_c+1}, K_{N_c+2}, \dots, K_N | \Omega | \Psi_{in} \rangle. \quad (2)$$

The linear operator A , which maps computational input states to computational output states, contains all the information of relevance to the transformation. We define the fidelity as the probability that the desired target gate A^{Tar} has been faithfully implemented on the computational modes given a successful measurement of the ancilla modes:

$$F(A) = \frac{|Tr(A^\dagger A^{Tar})|^2}{2^{M_c} Tr(A^\dagger A)}, \quad (3)$$

since $Tr(A^{Tar\dagger} A^{Tar}) = 2^{M_c}$ for a properly normalized target gate. As we are interested in deviations from perfect fidelity, we define $\delta = 1 - F$ as our main parameter [Smith11].

We define the success rate of the ancilla measurement to be given by an average over all computational input states,

$$S(A) = \frac{Tr(A^\dagger A^{Tar})}{2^{M_c} \|U\|^2}, \quad (4)$$

for general complex U . Note that U need not be unitary, as any matrix can be made unitary via the unitary dilation technique by adding vacuum modes [Knill02, uskov09]. We also note that the Hilbert-Schmidt norm $\langle A|A \rangle = Tr(A^\dagger A)/2^{M_c}$, used in our definition of S , is bounded above by the square of the operator norm, $\|A\|^2 = (\|A\|^{max})^2 = Max(\langle \Psi_{in}^{comp} | A^{Tar\dagger} A | \Psi_{in}^{comp} \rangle)$ and below by $(\|A\|^{min})^2 = Min(\langle \Psi_{in}^{comp} | A^{Tar\dagger} A | \Psi_{in}^{comp} \rangle)$ where the maximum and minimum are taken over the set of properly normalized input states. In the limit $F \rightarrow 1$, $\|A\|^{max}/\|A\|^{min} \rightarrow 1$, and all definitions of the success rate coincide.

3.4 Nonlocality, entanglement witnesses and supra-correlations

While entanglement is believed to underlie the power of quantum computation and communication, it is not generally well understood for multipartite systems. Recently, it has been appreciated that there exists proper no-signaling probability distributions derivable from operators that do not represent valid quantum states. Such systems exhibit *supra-correlations* that are stronger than allowed by quantum mechanics, but less than the algebraically allowed maximum in Bell-inequalities (in the bipartite case). Some of these probability distributions are derivable from an entanglement witness W , which is a non-positive Hermitian operator constructed such that its expectation value with a separable quantum state (positive density matrix) ρ_{sep} is non-negative (so that $Tr[W \rho] < 0$ indicates entanglement in quantum state ρ). In the bipartite case, it is known that by a modification of the local no-signaling measurements by spacelike separated parties A and B , the supra-correlations exhibited by any W can be modeled as derivable from a physically realizable quantum state ρ . However, this result does not generalize to the n -partite case for $n > 2$. Supra-correlations can also be exhibited in 2- and 3-qubit systems by explicitly constructing “states” O (not necessarily positive quantum states) that exhibit PR correlations for a fixed, but arbitrary number, of measurements available to each party. In this area of research we examined the structure of “states” that exhibit supra-correlations. In addition, we examined the affect upon the distribution of the correlations amongst the parties involved when constraints of positivity and purity are imposed. We investigated circumstances in which such “states” do and do not represent valid quantum states.

Physics imposes limits on the correlations that can be observed by distant (i.e. spacelike separated) parties. In particular, special relativity (SR) implies the principle of no-signaling (NS), that is correlations cannot lead to any sort of instantaneous communication between spacelike separated observers. Quantum correlations may be stronger than classical, and their violation of Bell inequalities (BI) [Bell64] suggest that quantum mechanics (QM) cannot be regarded as a local realism theory. Tsirelson [Tsirelson80] showed that there is an upper bound to the violation of BI, which implies that the amount of non-locality allowed by QM is limited. Popescu and Rohrlich (PR) showed [Popescu94] that there exists a broad class of no-signaling theories which allow stronger-than-quantum or supra-quantum correlations. PR developed a valid joint probability distribution whose violation of the BI lie above those of physical quantum correlations and below the allowed algebraic maximum of the BI (the latter are called PR-Boxes). Thus, the principle of NS imposed by SR does not single out QM from these other post-quantum NS theories [Masanes06] (PQNS).

These PQNS have much in common with QM such as no-cloning, information-disturbance tradeoffs, security for key distribution, and others. Recently, van Dam [van Dam05] showed that PR-Boxes make communication complexity trivial, which is not the case within QM. Other researchers have shown that PQNS theories would lead to implausible simplification of distributed computational tasks (see [Pawlowski09] and references therein). It is now widely believed that theories in which communication/computational complexity is trivial are very unlikely to exist. It is therefore important to understand the structure of the PQNS and ultimately to find physical and informational principles that rule them out. In this area of research we took steps in that direction by investigating the structure of PR correlations by forming operators which reproduce these PR probability distributions. We investigated circumstances in which they do and do not represent valid quantum states.

Bell Inequalities (BI)

Nonlocality is expressed by means of violations Bell inequalities¹ (BI) which set upper bounds for classical correlations arising from local-realistic theories. For bipartite systems, the most well know BI is the Clauser-Horne-Shimony-Holt (CHSH) inequality⁷ defined as follows. Consider a bipartite system $A \otimes B$, Alice and Bob, each possessing measurement directions $A, B = A$ and $C, D = B$ taking measurement values $a, b, c, d = \{\pm 1\}$. We define the correlation $E(AC)$ between $A=A$ and $C=B$ as

$$\begin{aligned} E(AC) &\equiv \langle AC \rangle = \sum_{a,c=\{\pm 1\}} a c P(a, c | A, C) \\ &= P(+, + | A, C) + P(-, - | A, C) - P(+, - | A, C) - P(-, + | A, C) \end{aligned} \quad (5)$$

In (5), we define $P(a, c | A, C)$ as the joint probability that given the (inputs) measurement directions A for Alice and C for Bob, Alice obtains the (outputs) measurement result a and Bob obtains the value b , subject to the normalization condition $\sum_{a,c=\{\pm 1\}} P(a, c | A, C) = 1, \forall A, C$. Finally, we define the following CHSH correlation parameter S by

$$S \equiv E(AC) + E(BC) + E(BD) - E(AD). \quad (6)$$

S has been cleverly constructed as the expectation value of the quantity $\text{Arg} \equiv A(C-D) + B(C+D)$. If A, B, C, D are classical random variables taking values ± 1 then it can be readily seen that if (i) $C=D$, then $|\text{Arg}| = |B(2C)| = 2$ and if (ii) $C=-D$, $|\text{Arg}| = |A(2D)| = 2$. Thus, for classical correlation we have the CHSH inequality

$$\text{CHSH inequality: } |S = E(AC) + E(BC) + E(BD) - E(AD)| \leq S_{cl} = 2 \quad (7)$$

(where the subscript “Cl” denotes “classical”). For a large class of measurement directions (but not all), quantum states can violate the CHSH inequality (i.e. $|S| > 2$) up to a maximum value shown by Tsirelson [Tsirelson80] to be $S_Q = 2\sqrt{2}$. Here, a *quantum state* is defined as a positive (i.e. non-negative eigenvalues) Hermitian matrix with unit trace denoted by the symbol ρ . The archetypical example is the singlet (Bell) state

$$\rho_{\text{singlet}} = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) / \sqrt{2} \equiv (|01\rangle - |10\rangle) / \sqrt{2} \quad (8)$$

with measurement directions in the x - y plane: $A = \hat{x}, B = \hat{y}, C = (\hat{x} + \hat{y})/\sqrt{2}, D = (\hat{x} - \hat{y})/\sqrt{2}$ that saturates the Tsirelson bound with $S = -S_Q = -2\sqrt{2}$. This is a manifestation of the stronger than classical correlations that can be exhibited by quantum states. (Note: quantum states with measurement directions such that the CHSH inequality is satisfied, i.e. $S \leq 2$, are not distinguishable from classical states by the correlation parameter S).

It is instructive to note that the CHSH inequality in (7) can be derived [Schumacher91] as a statement of a classical quadrilateral inequality for the *correlation metric* $\Delta(AC) = 1 - E(AC) = P(+, - | A, C) + P(-, + | A, C) \geq 0$. Substituting this expression into (7) yields $\Delta(AC) + \Delta(BC) + \Delta(BD) \geq \Delta(AD) \Rightarrow S \equiv E(AC) + E(BC) + E(BD) - E(AD) \leq +2$ (see Figure 10). Thus, the

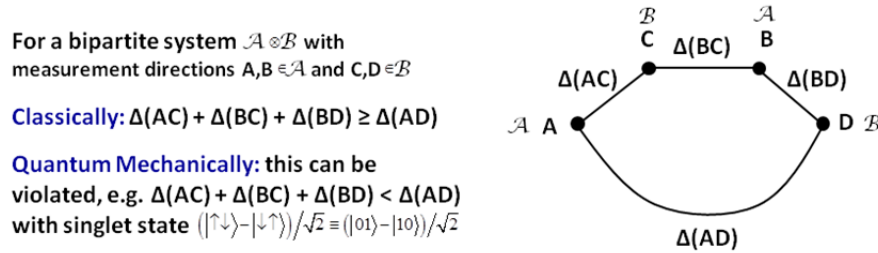


Figure 10. CHSH inequality derived as a violation of the classical quadrilateral inequality.

violation of the CHSH inequality by quantum states can be interpreted as a violation of the classical quadrilateral inequality which, for certain measurement directions, yields the distance $\Delta(AD)$ via the direct path A - D to be *smaller* than the sum of the distances around the indirect path A - C - B - D .

Returning to the CHSH inequality (7), one notes that it is bounded by the algebraic maximum $|S| \leq S_{AM} = 4$. This follows from the fact that the correlations E are bounded by $|E| \leq 1$. This latter result can be inferred by writing $E = P_{++} + P_{--} - (P_{+-} + P_{-+}) = 2(P_{++} + P_{--}) - 1 = 1 - 2(P_{+-} + P_{-+})$, where $P_{++} + P_{--} + P_{+-} + P_{-+} = 1$ has been used. Using the fact that $0 \leq P_{++} + P_{--} \leq 1$ and $0 \leq P_{+-} + P_{-+} \leq 1$ in the previous two expressions for E , yields the desired bound $|E| \leq 1$. Therefore, if the

first three correlations in (7) take the value ± 1 and the last correlation takes the value ∓ 1 , we obtain $S = \pm 4$. The implication of this observation is that the regime $2\sqrt{2} \leq S \leq 4$ represents *supra-correlations* that are stronger than quantum, yet are unphysical by Tsirelson's bound, i.e. cannot be realized by any physical quantum state. The salient question to study is what 'natural' principles determine the exclusion of such supra-correlations. As a first hypothesis, one might surmise that the principle of *no-signaling* from special relativity (i.e. that information cannot be instantaneously broadcast between spacelike separated observers) might exclude supra-correlations. Surprisingly, this is *not* the case. In 1994, Popescu and Rohrlich (PR) [Popescu94] were able to construct a valid joint probability distribution between a pair of spacelike separated observers that (i) satisfies the non-signaling principle, and (ii) yields the algebraic maximum correlations allowed by the CHSH inequality. Here the adjective 'valid' implies that the joint probability distribution, and all its derived marginal probability distributions, obtain values between 0 and 1, and satisfy the appropriated normalization requirements (i.e. the joint and all marginal probability distributions summed over all outcomes for any measurement settings yields unity). These correlations are now called *PR correlations*, which we describe in the next section.

No Signaling (NS) Theories and PR Correlations

We wish to consider correlations between n spacelike separated parties (observers) A_1, \dots, A_n , who can perform m possible measurements x_1, \dots, x_n ($x_i = \{0, 1, \dots, m-1\}$), with r possible outcomes a_1, \dots, a_n ($a_i = \{0, 1, \dots, r-1\}$). The observed correlations will be described by the joint probability distribution $P(a_1, a_2, \dots, a_n | x_1, \dots, x_n)$ giving the probability that the parties obtain the measurement values (outputs) a_1, \dots, a_n when their local measurement apparatuses (inputs) are set to x_1, \dots, x_n . The joint probability distribution is constrained only by the conditions $0 \leq P(a_1, a_2, \dots, a_n | x_1, \dots, x_n) \leq 1$ and the normalization condition $\sum_{a_1, \dots, a_n} P(a_1, a_2, \dots, a_n | x_1, \dots, x_n) = 1$ for all measurement settings x_1, \dots, x_n .

Imposing the no-signaling (NS) constraint, i.e. adherence to the requirement from special relativity that spacelike separated measurements should not influence each other due to the finite speed of light (communication), requires that the marginal probability distributions satisfy the additional condition

$$\text{No Signaling: } P(a_1, a_2, \dots, a_k | x_1, \dots, x_n) \equiv \sum_{a_{k+1}, \dots, a_n \in \{0, 1\}} P(a_1, \dots, a_n | x_1, \dots, x_n) = P(a_1, a_2, \dots, a_k | x_1, \dots, x_k). \quad (9)$$

Here, the first equality in (9) formally defines the marginal probability distribution describing the measurement outcomes of the first k parties, when the last $n-k$ outcomes are un-observed and hence summed over. Note, this marginal probability distribution $P(a_1, a_2, \dots, a_k | x_1, \dots, x_n)$ formally depends on all n measurement settings. The last equality in (9) imposes the NS constraint requiring that the marginal probability depends *only* upon the k measurement settings of the parties participating in the joint measurement (and not on the remaining $n-k$ measurement setting of the unobserved outcomes).

As first pointed out by Popescu and Rohrlich [Popescu94], the NS constraint (9) by itself does not single out classical and quantum theories, i.e. $|S| \leq S_Q$. PR proposed the following joint

probability distribution for two parties (Alice and Bob) with two measurement settings (inputs) $x, y = \{0, 1\}$, and two measurement outcomes (outputs) $a, b = \{0, 1\}$ given by

$$\text{PR Box: } P(a, b | x, y) = \begin{cases} 1/2 & \text{if } a \oplus b = x \cdot y \\ 0 & \text{otherwise} \end{cases}. \quad (10)$$

By considering all possible inputs and outputs, it is straightforward to show that PR correlations of (10) satisfy all the requirements for a NS theory as follows: normalization (total probability)

$$\begin{aligned} & \sum_{a, b \in \{0, 1\}} P(a, b | x, y) \\ &= \underbrace{P(0, 0 | x, y) + P(1, 1 | x, y)}_{a \oplus b = 0} + \underbrace{P(0, 1 | x, y) + P(1, 0 | x, y)}_{a \oplus b = 1}, \\ &= (1/2 + 1/2) \delta_{0, x \cdot y} + (1/2 + 1/2) \delta_{1, x \cdot y}, \\ &= \delta_{0, x \cdot y} + \delta_{1, x \cdot y}, \\ &= 1 \quad \forall x, y, \end{aligned} \quad (11)$$

and the NS constraint

$$\begin{aligned} P(a | x, y) &\equiv \sum_{b \in \{0, 1\}} P(a, b | x, y) \\ &= \underbrace{P(a, 0 | x, y)}_{a \oplus b = a \oplus 0 = a} + \underbrace{P(a, 1 | x, y)}_{a \oplus b = a \oplus 1 = \bar{a}} \\ &= 1/2 \delta_{a, x \cdot y} + 1/2 \delta_{\bar{a}, x \cdot y}, \\ &= \begin{cases} 1/2 + 0 & (\text{if } a = 0 \& x \cdot y = 0), 0 + 1/2 & (\text{if } a = 0 \& x \cdot y = 1) \\ 0 + 1/2 & (\text{if } a = 1 \& x \cdot y = 0), 1/2 + 0 & (\text{if } a = 1 \& x \cdot y = 1) \end{cases}, \\ &= 1/2 \quad \forall a, x, y, \\ &= P(a | x) \quad \forall a, x \quad (\Rightarrow \text{Isotropic, i.e. } P(a | x) = 1/2 \text{ indep of } a, x). \end{aligned} \quad (12)$$

With the PR Box define above in (10) we can compute correlations as

$$\begin{aligned} E(a, b | x, y) &= \underbrace{P(0, 0 | x, y) + P(1, 1 | x, y)}_{a \oplus b = 0} - \underbrace{P(0, 1 | x, y) + P(1, 0 | x, y)}_{a \oplus b = 1}, \\ &= (1/2 + 1/2) \delta_{0, x \cdot y} - (1/2 + 1/2) \delta_{1, x \cdot y}, \\ &= \begin{cases} +1 & \text{if } x \cdot y = 0, \text{ i.e. } (x, y) \in \{(0, 0), (0, 1), (1, 0)\}, \\ -1 & \text{if } x \cdot y = 1, \text{ i.e. } (x, y) = (1, 1), \end{cases} \end{aligned} \quad (13)$$

where we have used $E(a, b | x, y) = \sum_{a', b' \in \{\pm 1\}} a' b' P(a, b | x, y)$, where $a' = 1 - 2a$ ($b' = 1 - 2b$) associates the measurement values $a' (b') \in \{+1, -1\}$ with the measurement value labels (bits) $a (b) \in \{0, 1\}$,

respectively. Therefore, in Figure 10, assigning Alice's measurement directions $A, B = A$ the bit labels $x_A=1$ and $x_B=0$, and Bob's measurement directions $C, D = B$ the bit labels $y_C=0$ and $y_D=1$, and using (6) yields the algebraic maximum $S_M=4$ of the CHSH inequality, as illustrated in Figure 11.

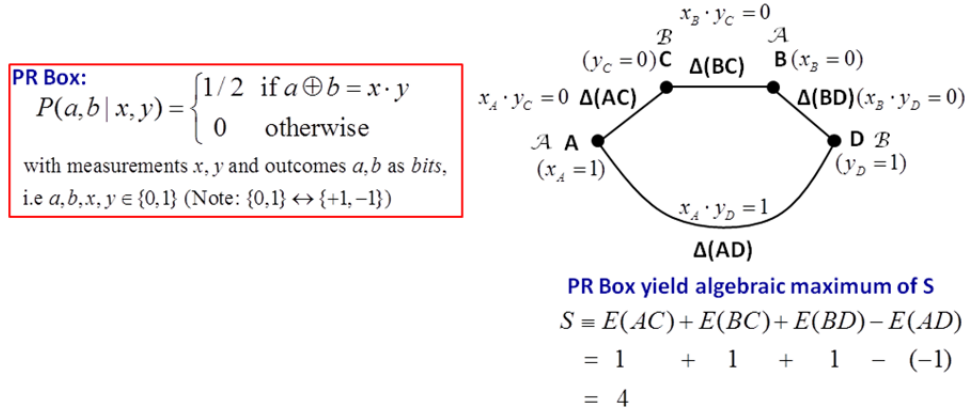


Figure 11. PR Box with joint probability distribution achieving the algebraic maximum $S_M=4$ of the CHSH inequality.

Since $S_M=4 > S_Q=2\sqrt{2}$, no quantum (i.e. physically realizable) state can reproduce the above PR probability (10). However, the following “state” [Acin10] $O = \alpha_+ |\Phi^+\rangle\langle\Phi^+| + \alpha_- |\Phi^-\rangle\langle\Phi^-|$ with $\alpha_{\pm} = (1 \pm \sqrt{2})/2$ and Bell states $|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, yields the PR probability (10) through the usual trace rule $P_{PR}(a, b | x, y) = \text{Tr}[O M_a^x \otimes M_b^y]$ with $\{M_a^{x_A}, M_a^{x_B}\} = \{\sigma_2, \sigma_1\}$ and $\{M_b^{y_C}, M_b^{y_D}\} = \{(\sigma_1 + \sigma_2)/\sqrt{2}, (\sigma_1 - \sigma_2)/\sqrt{2}\}$, where $\{\sigma_i\}_{i \in \{1, 2, 3\}}$ are the usual Pauli matrices. Note that the form of the joint measurement between Alice and Bob written as a pure tensor product of local observables $M_a^x \otimes M_b^y$, ensures the locality of the spacelike separated measurements, which cannot increase entanglement between the parties. (A measurement involving the sum of pure tensor products, such as $M_a^x \otimes M_b^y + M_a^{x'} \otimes M_b^{y'}$ which might possibly create entanglement, would involve non-local measurements between the parties, which could only be physically realized if the parties were brought together). The important point is that O does not represent a physical quantum state since it is non-positive, i.e. it possesses the negative eigenvalue $\alpha_- = (1 - \sqrt{2})/2$. Henceforth, we shall refer to non-positive, unit trace Hermitian operators O capable of producing NS probability distributions as “states,” and reserve the specific term “quantum state” or “q-state” for the physically realizable positive, unit trace Hermitian operators denoted as $\rho \geq 0$, (i.e. density matrix).

Following Acin *et al.* [Acin10] we desired to investigate all sets of n -party spacelike correlations in terms of local quantum observables (measurements) $M_{\text{non-sig}} = M_{a_1}^{x_1} \otimes \dots \otimes M_{a_n}^{x_n}$ that ensure NS.

These correlations can be written in the form

$$P_O \equiv P_O(a_1, \dots, a_n | x_1, \dots, x_n) = \text{Tr}[O M_{a_1}^{x_1} \otimes \dots \otimes M_{a_n}^{x_n}]. \quad (14)$$

Without loss of generality, we can take the local measurement operators $M_a^x = \Pi_a^x = |a\rangle_x \langle a|$ to be the projection operators onto “spin-component” a in the “direction” x . Requiring that proper probabilities be derived from *all* local quantum measurements imposes the condition that O be positive on *all* product states. This implies that $O=W$ is an entanglement witness (EW, see [Guhne09]) with the property $\langle \alpha, \beta, \dots | W | \alpha, \beta, \dots \rangle \geq 0$. Here some definitions are helpful. A q-state is separable (contains only classical correlations) if it is of the form $\rho^{sep} = \sum_i p_i \rho_i^{A_1} \otimes \rho_i^{A_2} \otimes \dots \otimes \rho_i^{A_N}$ where each $\rho_i^{A_i}$ is a local density matrix and $\sum_i p_i = 1$. (If a q-state is not separable, it is entangled). Each local density matrix has a (non-unique) ensemble decomposition $\rho_i^{A_k} = \sum_j p_{ij}^k |\psi_{ij}^k\rangle \langle \psi_{ij}^k|$ where $\sum_j p_{ij}^k = 1$. The requirement that W is positive on all product states $\langle \alpha, \beta, \dots | W | \alpha, \beta, \dots \rangle \geq 0$ ensures that $Tr[\rho^{sep} W] \geq 0$ from the form of ρ^{sep} . A q-state ρ such that $Tr[\rho W] < 0$ is then entangled (since it is not separable), and W is said to “witness” (or exhibit) the entanglement of ρ . Note that W is in general a non-positive Hermitian operator. In the context of (10), we now consider $O \rightarrow W$ as a state (not necessarily a q-state) from which to derive NS correlations through the joint probability distributions

$$P_W \equiv P(a_1, \dots, a_N | x_1, \dots, x_N) = Tr[W M_{a_1}^{x_1} \otimes \dots \otimes M_{a_N}^{x_N}] \geq 0. \quad (15)$$

The correlations (15) are termed *Gleason correlations* by Acin *et al.* [Acin10].

The subtle distinction between (14) and (15) is that the latter produces positive probabilities for *all* local NS measurements, while the former may produce non-negative probabilities on only a *subset* of NS measurements. This distinction is important since it has been shown [Guhne09, Barnum10] that for bipartite systems $n=2$, any Gleason correlation $P(a_1, a_2 | x_1, x_2) = Tr[W M_{a_1}^{x_1} \otimes M_{a_2}^{x_2}] \geq 0$ can be converted to a probability distribution derived from a q-state $\rho_{|\Phi_{PB}\rangle} = |\Phi_{PB}\rangle \langle \Phi_{PB}|$ with modified measurements $P(a_1, a_2 | x_1, x_2) = Tr[W M_{a_1}^{x_1} \otimes M_{a_2}^{x_2}] = Tr[\rho_{|\Phi_{PB}\rangle} M_{a_1}^{x_1} \otimes \bar{M}_{a_2}^{x_2}] \geq 0$. Here $|\Phi_{PB}\rangle$ is any pure bipartite state (not necessarily maximally entangled). The proof relies on the explicit use of the Choi-Jamiołkowski isomorphism (CJI) [Guhne09, Barnum10, Vedral97] which allows any bipartite ($n=2$) witness W to be written as $W^{(n=2)} \equiv (I \otimes \Lambda)(\rho_{|\Phi_{BP}\rangle})$, where Λ is a positive trace preserving map. In the above, $\bar{M}_{a_2}^{x_2} = \Lambda^*(M_{a_2}^{x_2})$ where Λ^* is the adjoint of the map Λ , i.e. $Tr[A \Lambda(B)] = Tr[\Lambda^*(A) B]$. The proof then follows directly as

$$\begin{aligned} P_W(a, b | x, y) &= Tr[W M_a^x \otimes M_b^y] = Tr[(I \otimes \Lambda)(\rho_{|\Phi_{BP}\rangle}) M_a^x \otimes M_b^y] \\ &= Tr[M_a^x \otimes M_b^y (I \otimes \Lambda)(\rho_{|\Phi_{BP}\rangle})] = Tr[M_a^x \otimes \Lambda^*(M_b^y) \rho_{|\Phi_{BP}\rangle}] = Tr[\rho_{|\Phi_{BP}\rangle} M_a^x \otimes \bar{M}_b^y], \end{aligned} \quad (16)$$

where the second equality uses the CJI, the third equality uses the cyclic property of the trace, the fourth inequality utilizes $I \otimes \Lambda$ acting to the left on the tensor product measurements $M_a^x \otimes M_b^y$ thereby introducing the adjoint Λ^* operation and the modified local measurement operation

$\bar{M}_{a_2}^{x_2} = \Lambda^*(M_{a_2}^{x_2})$ in the last equality. Acin *et al.* [Acin10] point out that the CJI decomposition $W^{(N=2)} \equiv (I \otimes \Lambda)(\rho_{|\Phi_{PR}\rangle})$ in general fails for $n > 2$ (which they demonstrate by a specific example). Thus, the Gleason correlations (15) are strictly larger ($|S| > S_Q$) than quantum correlations for $n > 2$ (and equivalent only for $n \leq 2$). The state $O = \alpha_+ |\Phi^+\rangle\langle\Phi^+| + \alpha_- |\Phi^-\rangle\langle\Phi^-|$ used in the example of PR correlations in the discussion after Figure 11 is *not* an EW since it can produce negative probabilities for measurements other than those considered (it would be an EW if it produced positive probabilities for *all* measurement choices). Acin *et al.* [Acin10] classify the distributions $P(a_1, \dots, a_n | x_1, \dots, x_n)$ as (i) *No-Signaling* if and only if P can be written in the form of (14), (ii) *Quantum* whenever O is positive ($O \geq 0$), and (iii) *Local* if and only if O corresponds to a separable quantum state. In the following, we investigate the NS correlations of (10) and the conditions for which they become either Gleason, or Quantum correlations.

3.5 Efficient Cluster State Generation

Entangled quantum states of light are in great demand in quantum technology today. Photonic quantum information processing, and metrology are all based on exploiting special properties of non-classical multipath entangled states. Due to their high robustness against decoherence, and relatively simple manipulation techniques, photons are often exploited as the primary carriers of quantum information. A generally accepted encoding scheme using photons is dual rail encoding, in which logical qubit states $|\uparrow\rangle$ and $|\downarrow\rangle$ are encoded in two-mode Fock states $|1,0\rangle$ and $|0,1\rangle$, respectively. In experimental photon implementations, these two modes are commonly associated with horizontal and vertical polarizations. An attractive feature of such an encoding is that single-qubit SU(2) operations can be performed by the standard techniques of linear optics, using practically lossless beam splitters and phase shifters. However, when it comes to entangling photon-encoded qubits, a problem immediately arises: the absence of a photon-photon interaction for coupling the photons.

Optical Kerr nonlinearity can effectively couple photons through their interaction with a dispersive medium. However due to the low photon numbers involved in typical quantum-information processing tasks, such nonlinearity is extremely weak and is of little practical use.

Alternatively, an effective photon-photon interaction may be produced using ancilla modes and projective measurements. A quantum state generator can then be realized utilizing only linear-optical elements (beam splitters and phase shifters) in combination with photon counters, at the expense of the process becoming probabilistic. The revolutionary discovery by Knill, Laflamme, and Milburn (KLM) [Knill01], launched the field of linear optical quantum information processing, was that such a device is capable of transforming an initially separable state into entangled state. Since the transformation depends on the success of the measurement, the transformation has a probabilistic nature.

The paradigm of quantum computation is based on peculiar laws of quantum mechanics which potentially allow manipulation and processing of information at exponentially faster rates as compared to classical computers. There exist at least two distinct schemes of implementing quantum computation. Historically the first scheme is based on the sequential application of a number of logical gates to elementary carriers of quantum information (qubits). The second scheme, discovered in 2001 by Hans Briegel and Robert Raussendorf [Raussenfor01], does not have a classical counterpart: it exploits the purely quantum phenomenon of wave function collapse under a measurement. A computation is performed by inducing non-unitary dynamics in a carefully prepared quantum state of multiple mutually entangled qubits by applying a sequence of measurements according to a desired computational algorithm. Such quantum states are called cluster states or, more generally, quantum graph states.

Since the cluster state paradigm offers better possibilities for error correction this scheme became the leading candidate for the physical realization of quantum information processing. From a physical point of view, photon based implementations of cluster states, where information is encoded in wave functions of single photons, has important advantages compared to other technologies.

Optical transformation by postselection in coincidence basis

The quantum measurement-assisted linear optical quantum computer was originally envisioned as a network of linear optical elements (for example in the original KLM scheme), where the controlled sign (C-phase or, equivalently, CZ) gate is constructed as a combination of two nonlinear sign (NS) gates. This approach was effective as a “proof of principle” for linear optical entangling transformations. However, for the technical purpose of building a functional microchip-based device, one does not need to partition the transformation into blocks. Instead, the device may be considered as an “integrated light circuit” which performs one large operation and one needs to make use of theoretical tools to optimize the fidelity, success, and robustness of the device for a given set of resources available in the form of ancilla photons.

First we shortly describe the general scheme of liner-optical transformation.

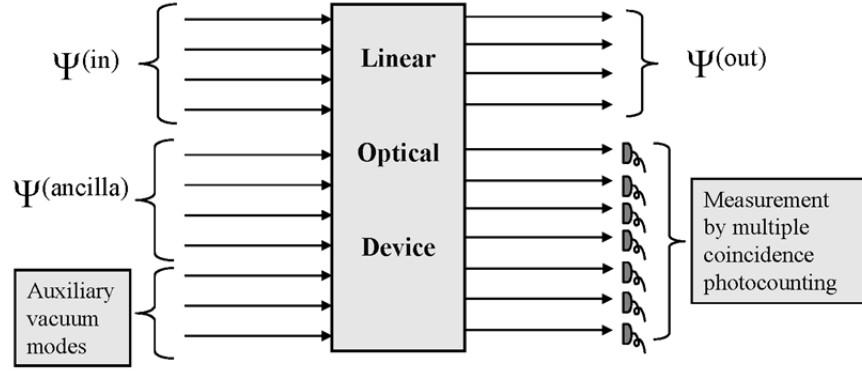


Figure 12. A general measurement-assisted transformation using a linear optical interferometer [VanMeter07]. The “computational” input state $\Psi^{(in)}$ is usually a separable state of two or more dual-rail encoded qubits. The ancilla state usually is assumed to be a separable state.

The core of the linear optical device is the transformation,

$$a_i^\dagger \rightarrow \sum_{j=1}^N U_{ij} \tilde{a}_j^\dagger \quad (17)$$

of the photon creation operators from the input to the output state. Here N is the total number of optical modes, and U is a unitary $N \times N$ matrix, which contains all physical properties of the linear optical device. The induced state transformation Ω is a high-dimensional unitary representation of the matrix U . Its action is given by the following algebraic operation on the input state $|\Psi^{(total\ input)}\rangle = |\Psi^{(in)}\rangle |\Psi^{(ancilla)}\rangle$,

$$|\Psi^{(total\ output)}\rangle = \Omega |\Psi^{(total\ input)}\rangle = \Omega \prod_{i=1}^N \frac{a_i^{\dagger n_i}}{\sqrt{n_i!}} |0\rangle = \prod_{i=1}^N \frac{1}{\sqrt{n_i!}} \left(\sum_j U_{ij} \tilde{a}_j^\dagger \right)^{n_i} |0\rangle \quad (18)$$

The map between operators $U \rightarrow \Omega$ is a group homomorphism, i.e. if $U_1 \rightarrow \Omega_1$ and $U_2 \rightarrow \Omega_2$ then $U_1 U_2 \rightarrow \Omega_2 \Omega_1$.

Next, a Von-Neumann measurement in the Fock basis is performed on a subspace of the final state $|\Psi^{(total\ output)}\rangle$ and only one measurement outcome is accepted as a successful implementation of the transformation. If the measurement involves only the set of ancilla modes, then mathematically this operation is equivalent to projecting the $|\Psi^{(total\ output)}\rangle$ state onto a predefined Fock state in the ancilla modes $|\Psi^{(mesurement)}\rangle = |k_{m+1}, k_{m+2}, \dots, k_N\rangle$.

$$\left| \Psi_{out}^{(comp)} \right\rangle = \left\langle k_{N_c+1}, k_{N_c+2}, \dots, k_N \right| \Omega \left| \Psi_{input}^{(comp)} \right\rangle = A \left| \Psi_{input}^{(comp)} \right\rangle. \quad (19)$$

Here A is a *contraction* Kraus linear operator [Kraus83] acting on the input computational state denoted above as $\left| \psi^{(in)} \right\rangle$. In the literature transformation (19) is called a measurement-assisted transformation or a Stochastic Local Operations and Classical Communication (the classical communication part is important only for schemes utilizing feed-forward technique to boost the success probability).

A special type of measurement-assisted transformation is achieved by merging computational and ancilla modes in the general scheme described above. For these transformations, photons in the computational modes are playing two roles at the same time: i) carriers of quantum information ii) generators of measurement-induced optical nonlinearities. In other words we get $\left| \Psi^{(in)} \right\rangle \equiv \left| \Psi^{(total\ input)} \right\rangle$.

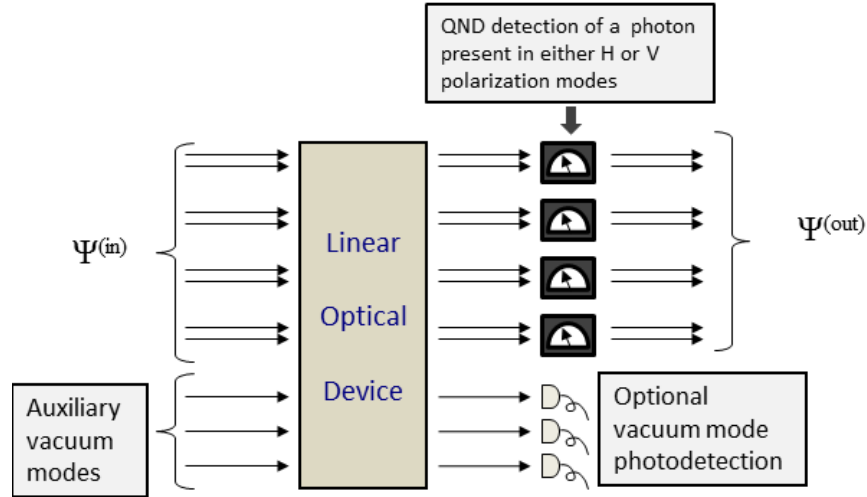


Figure 13. State transformation where photo-detection is used to detect the presence of a photon in either one of two modes of a dual-rail pair. Since this type of measurement does not induce a complete collapse of the wave function it will not destroy quantum information encoded in computational dual-rail subspaces including any form of multiqubit entanglement.

To introduce a proper mathematical description of such schemes we first need to discuss the notion of dual-rail encoding. Contrary to single-rail encoding, when qubit logical states $|0\rangle$ and $|1\rangle$ are encoded in vacuum and one-photon states correspondingly, in dual-rail encoding logical states $|0\rangle$ and $|1\rangle$ are represented by horizontal $|H\rangle$ and vertical $|V\rangle$ polarizations of one spatial mode. From the mathematical point of view horizontal and vertical modes are equivalent to any two orthogonal (spatial) modes since linear optical transformations of photon creation operators of input modes can be equally implemented for polarization rotations and transformations between modes. Therefore dual-rail encoding in general involves two abstract photonic modes

and the qubit Hilbert space is simply the single-photon eigenspace of the photon number operator $\hat{N} = a_1^\dagger a_1 + a_2^\dagger a_2$. Denoting as $|H, V\rangle_n$ the states with horizontal and vertical polarization in the n -th spatial mode can be written in the multiqubit space as $\text{span}(\prod_{n=1}^N |H, V\rangle_n)$. Now instead of a projection on the ancilla state, as in equation (19), the Von-Neumann measurement is represented by the projection operator on the computational basis $\hat{\mathbf{P}}^{(comp)} = \sum_{n=1}^N (|H\rangle_n \langle H|_n + |V\rangle_n \langle V|_n)$, and equation (19) takes the form,

$$|\psi^{(out)}\rangle = \hat{\mathbf{P}}^{(comp)} \mathbf{\Omega} |\psi^{(in)}\rangle = \mathbf{A} |\psi^{(in)}\rangle. \quad (20)$$

In principle, the operation (20) implies the application of a quantum non-demolition (QND)-type device which detects the presence of a photon in two modes without disturbing its quantum state. However, such a requirement can be eliminated in the cluster model of quantum computation when the read-out operation is nothing else but a multiqubit measurement in the basis of qubit product states. Such elimination imposes certain restrictions on the possibility of concatenating linear optical transformations, defined by equation (1), which we will discuss in detail elsewhere.

Describing the quantitative properties of transformations (20) we first clarify a common misconception concerning “transformations” and “gates”. The latter is always a unitary operator while the former in general is not (more mathematical details can be found in texts on semi-groups). A special class of transformations (19) or (20) generating matrices \mathbf{A} such that $\mathbf{A} \mathbf{A}^\dagger = s \hat{I}$, $s \in R$ are called “operational unitary”. The parameter s in this relation is simply the success probability of the transformation. Transformations of this type can simulate a unitary gate, such as the CNOT gate, for example. There is a significant body of work dedicated to the optimization of such transformations. However in the present paper the focus of our study is on how such transformations act on specific states, i.e. we are interested only in the action of such transformations on a special input state which is taken to be either a product of single-qubit states or a product of Bell states.

Fidelity and success probability of optical measurement-assisted transformation of a quantum state

We introduce two important characteristics of state transformation which determine the usefulness of a transformation for generating a desired (or target) state $|\psi^{(tar)}\rangle$.

The first characteristic of the state transformation quantifies how close the “out-state” $|\psi^{(out)}\rangle$ is to the target state $|\psi^{(tar)}\rangle$, is called the fidelity of the transformation. Fidelity is defined in terms of the standard Fubini-Study distance

$$\gamma(\psi^{(out)}, \psi^{(tar)}) = \cos^{-1} \left(\sqrt{\langle \psi^{(out)} | \psi^{(tar)} \rangle \langle \psi^{(tar)} | \psi^{(out)} \rangle} / \sqrt{\langle \psi^{(out)} | \psi^{(out)} \rangle \langle \psi^{(tar)} | \psi^{(tar)} \rangle} \right) \quad (21)$$

Here $|\psi^{(tar)}\rangle$ is the state given by equation (20). For numerical computations it is expedient to accept the following non-singular parameter as the measure of fidelity: two states have zero distance γ if parameter

$$f(\mathbf{U}) = \left| \langle \psi^{(out)} | \psi^{(tar)} \rangle \right|^2 / \langle \psi^{(out)} | \psi^{(out)} \rangle \equiv \cos(\gamma)^2 = 1 \quad (22)$$

is equal to one. If the measurement results in a desired outcome the transformation will produce a “collapsed” normalized state $|\hat{\psi}^{(out)}\rangle = |\psi^{(out)}\rangle / \sqrt{\langle \psi^{(out)} | \psi^{(out)} \rangle}$ and the condition of unit fidelity ($f=1$) guarantees that $|\hat{\psi}^{(out)}\rangle = e^{i\phi} |\psi^{(tar)}\rangle$ (i.e. the target and out-state differ only by a global phase).

Technically the most important characteristic of a measurement-assisted transformation is the value of the success probability of the transformation. While for the gate optimization problem success probability is usually introduced as the Hilbert-Schmidt norm of the operator \mathbf{A} : $s = \text{Tr}(\mathbf{A}\mathbf{A}^\dagger) / D_c$, where D_c is the dimensionality of the Hilbert space, the success probability of the state transformation can be defined simply as a normalization matrix element

$$s(\mathbf{U}) = \langle \psi^{(out)} | \psi^{(out)} \rangle \equiv \langle \psi^{(in)} | \mathbf{A}^\dagger \mathbf{A} | \psi^{(in)} \rangle \equiv \langle \psi^{(in)} | \boldsymbol{\Omega} \hat{\mathbf{P}}^{(comp)} \boldsymbol{\Omega} | \psi^{(in)} \rangle. \quad (23)$$

The goal of the current study is to find the linear optical matrix \mathbf{U} which provides the largest possible success probability $s(\mathbf{U})$ with perfect fidelity ($f(\mathbf{U})=1$) for generating linear cluster states from single-qubit product states or two-qubit Bell states. Mathematically, both $s(\mathbf{U})$ and $f(\mathbf{U})$ are real-valued functions on the compact $\text{SU}(N)$ manifold of unitary operators \mathbf{U} and the problem of finding a global maximum of $s(\mathbf{U})$ while keeping perfect fidelity belongs to the category of restricted optimization problems. The numerical implementation of the optimization problem in the present study is similar to technique developed for gate optimization, where technical details of the optimization code are described. The main feature of the numerical optimization routine which is important for the present paper is that global optimization is pursued by implementing multiple cycles of local optimization with varying starting points and then plotting and analyzing the data for local maxima in the increasing order of success rate.

4.0 RESULTS AND DISCUSSION

4.1 Multipli-entangled photons from a spontaneous parametric down-conversion source

Experimental analysis and testing apparatuses for Schioedtei are very similar to that for any SPDC source. With the more complex ring pattern generated though there are modifications one must do to the standard detection scheme. The experimental configuration for Schioedtei is shown in Figure 14. The testbed consists of a violet (405 nm) femtosecond pulsed pump source (Millenia PRO 15sJ > Tsunami 3960-15HP > Inspire Blue FM) with an average power of ~ 1.4 W, ~ 100 femtosecond pulses and a repetition rate of 80 MHz. The 405 nm pulses first pass through a ~ 12.5 mm quartz pre-compensator and a half-wave plate set to 22.5° to rotate the input linear polarization to the required 45° for equal excitation of the crystals before entering Schioedtei. Proper alignment of the crystal was accomplished with live images from a cooled CCD camera (Princeton Instruments Pixis 1024BR). The photons were collected in free space collimators located 1.5 meters behind Schioedtei. This distance is the minimum amount required to obtain the useable spatial separation required for detector access to the middle blue diamond of intersection points (5, 6, 7, and 8). The post-compensating crystals, inserted in the down-converted photon paths, are $8 \times 8 \times 1$ mm type II phase matched β -BBO (at angles of $\theta = 41.9^\circ$ and $\phi = 30^\circ$) as Schioedtei's orientation is non-collinear and there is no interaction between the pump and the compensators. These compensators could not be used for compensation of a collinear configuration as they were phase matched for SPDC at 810 nm when exposed to a 405 nm excitation beam. Photon collection was accomplished via fiber coupled collimators immediately

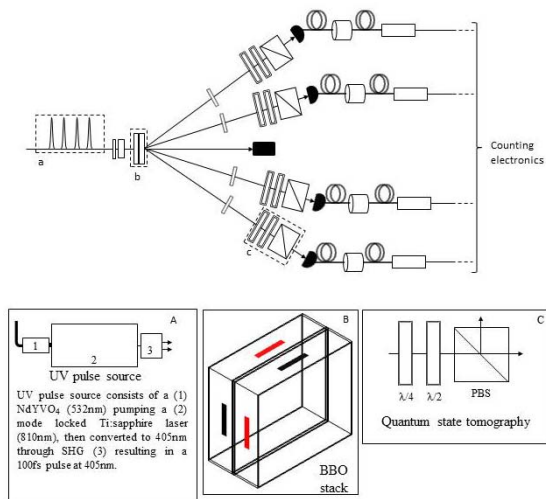


Figure 14. Experimental testbed to analyze the Schioedtei source.

followed by 2 nm bandpass filters. The output of the bandpass filter was routed directly into fiber-coupled single photon counting avalanche photodiodes (APDs) (Perkin Elmer SPCM-AQ4C). Coincidence detection was accomplished by a four channel coincidence counting module (CCM) [Branning11].

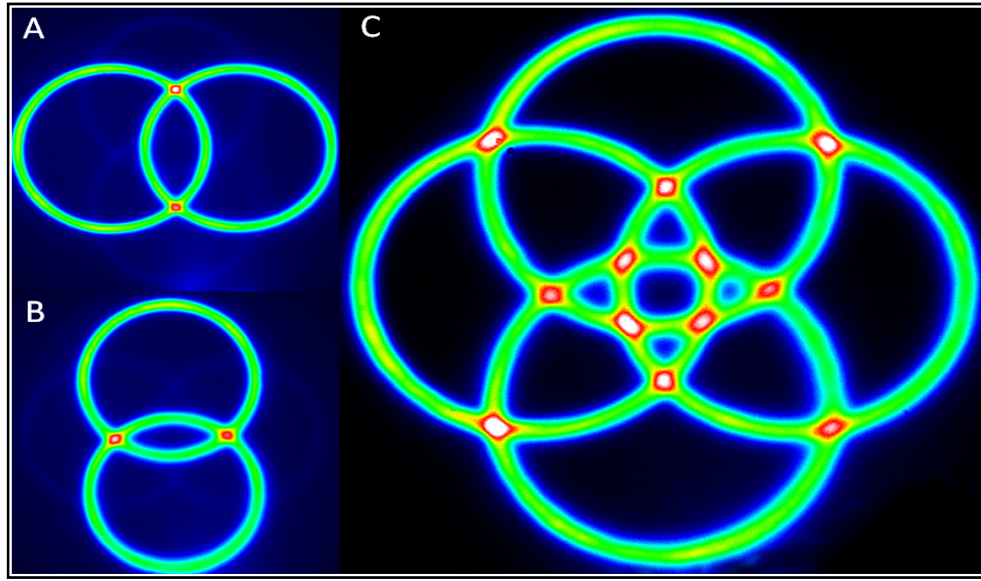


Figure 15. False color CCD images of custom crystal assembly (1 sec exposure). A,B are the type II non-collinear outputs from each individual crystal. C is the combined output from the crystal stack.

A trio of false color CCD camera images of Schioedtei output is shown in Figure 15. The twelve overlap regions are clearly visible and the spatial symmetry of the output should be clearly noted. The orientation of the crystal assembly gives an approximate Gaussian profile on spots 5,6,7,8 and a slightly elongated profile for spots 1,2,3,4,9,10,11,12. The alignment image in Figure 16 is utilized for aligning the proper orientation of the rings while a back propagated beam shown in Figure 16 aligns the collimators to the intersection points.

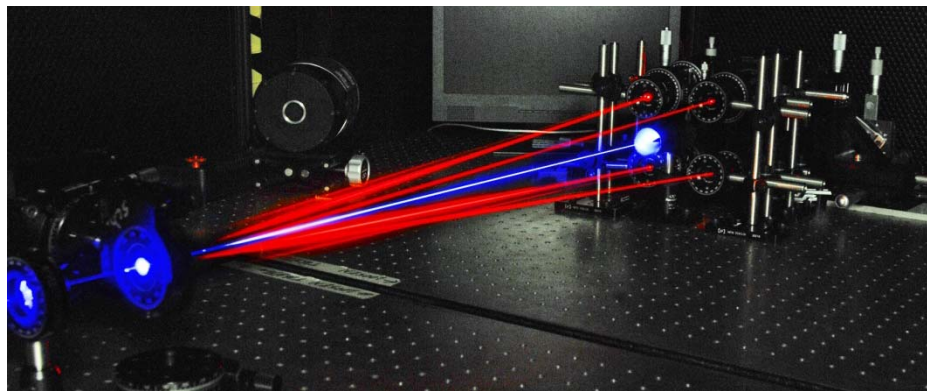


Figure 16. Alignment image of the Schioedtei crystal stack.

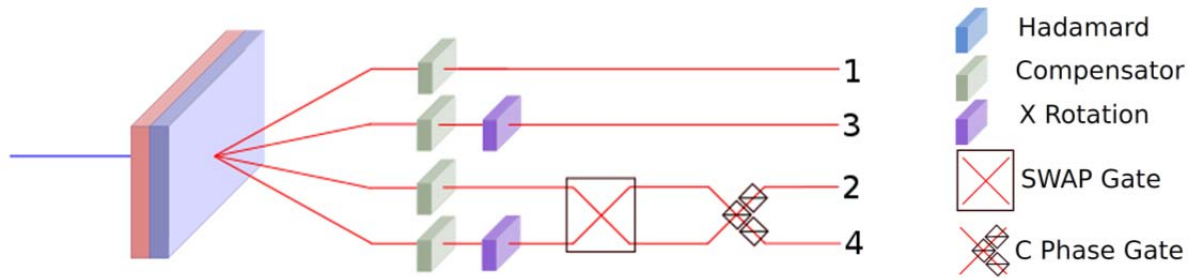
As stated, Schioedtei was constructed from β -BBO though any type II material can be used. Materials such as BiBO (Bismuth Borate, BiB_3O_6) have been shown to have a higher photon generation rate than β -BBO [Rangarajan09] and this will be the next step for Schioedtei. Secondly, increasing the useable photon count rate in Schioedtei can be accomplished by factoring the GVM phase matching constraint [U'Ren06] into the crystal construction. A GVM-matched configuration [Fanto10] is possible by alternating reduced thickness Schioedtei and α -

BBO layers. α -BBO can be used as a compensator since there is no second order nonlinear effect in α -BBO crystal due to the centric symmetry in its crystal structure. Such a GVM source would provide the same up to six spatially separate entangled pairs as Schioedtei, while alleviating the need for spectral filtering of the photons. An increase in useable signal rates of 10x over a typical type II source is realizable with GVM matching.

Schioedtei source uses and applications

Another applicable area of extreme interest is in the generation of photon-based cluster states. Cluster states play a central role in the measurement-based one-way quantum computation approach [Walther05, Raussendorf01]. In this scheme, the entanglement resource is provided in advance through an initial, highly entangled multi-qubit cluster state and is consumed during the quantum computation by means of single-particle projective measurements. The feedforward nature of the one-way computation scheme renders the quantum computation deterministic, and removes much of the massive overhead that arises from the error encoding used in the standard quantum circuit computation model [O'Brien07]. Figure 17 illustrates a scheme for utilizing the output of Schioedtei to generate a four photon cluster state, $|C\rangle_4$ [Schmid07]. This particular example employs the spots 1,2,3,4 and requires insertion of two half-wave plates, a SWAP gate and a controlled-phase (CPhase) gate. This scheme could be expanded to include the other eight spots to generate even larger cluster states. Such experiments are currently being explored in-house.

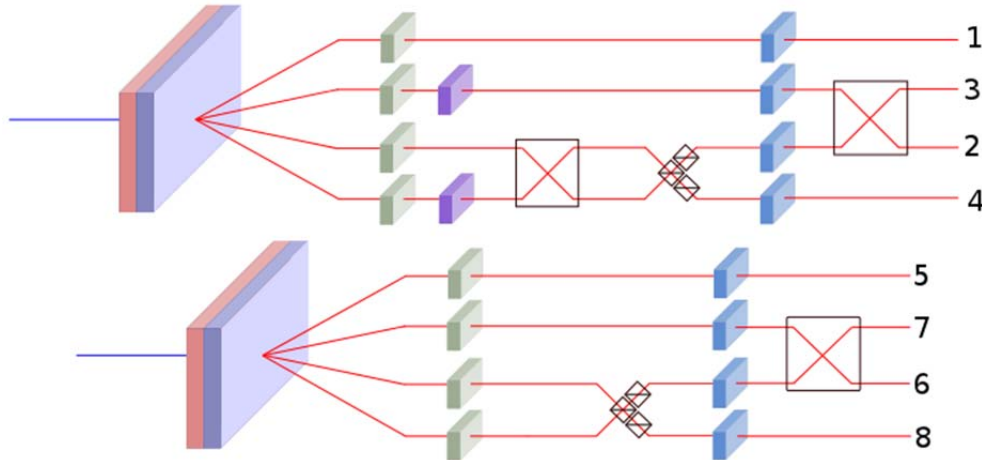
More complex cluster states can be constructed from Schioedtei with additional hardware. This includes, but is not limited to, the construction of box cluster states [Prevedel07, Walther05]. In fact Schioedtei is capable of producing two 4 qubit box states simultaneously by using 8 of the spots; 1,2,3,4 and 5,6,7,8. As the states Schioedtei outputs at these 2 sets of spots are different,



$$|C\rangle_4 = \frac{1}{2} (|HHHH\rangle_{1,2,3,4} + |HHVV\rangle_{1,2,3,4} + |VVHH\rangle_{1,2,3,4} - |VVVV\rangle_{1,2,3,4})$$

Figure 17. Experimental setup for 4-qubit cluster state generation utilizing Schioedtei.

slightly different preparation methods are required for the two boxes, as shown in Figure 18. After the preparation is complete the two box states are completely equivalent. With additional preparation and resource photons these states can be used as the building blocks of larger states such as the 6 qubit butterfly network [Ma10, Soeda10].



$$|\psi\rangle_{\text{BOX}} = \text{Swap}_{2,3} H_1 H_2 H_3 H_4 \text{CZ}_{2,4} \text{Swap}_{2,4} X_3 X_4 |\psi\rangle_{1,2,3,4}$$

$$|\psi\rangle_{\text{BOX}} = \text{Swap}_{6,7} H_5 H_6 H_7 H_8 \text{CZ}_{6,8} |\psi\rangle_{5,6,7,8}$$

Figure 18. Experimental construction of a 4-qubit box cluster state utilizing Schioedtei.

An advantage of the Schioedtei configuration is the diversity of states that it is capable of generating. Schioedtei allows for the direct generation of the (unnormalized) state $|HV\rangle \pm e^{i\varphi}|VH\rangle$ along with the generation of the state $|HH\rangle \pm e^{i\varphi}|VV\rangle$ with the addition of a half-wave plate. In addition, separable states such as $|HV\rangle \pm e^{i\varphi}|VV\rangle$ or $|HV\rangle \pm e^{i\varphi}|HH\rangle$ can also be directly generated with clever combinations of the twelve output intersections and proper compensation.

4.2 A path towards experimental generation of a linear cluster states (5 Figs: 19-23)

A successful detection of two pairs of entangled photons is reported along with several implemented updates to the experimental quantum information science test bed. First, a new photon collection system was created and installed in order to create a smaller footprint, move collimators closer to the source, and reduce the number of variables involved in finding the optimum collimator location to collect entangled photons. The final configuration is depicted in figure 19. The photon collection apparatus constructed is easily adapted for type I or II down conversion rings or Schioedtei rings. The four mirrors with a smaller footprint than the collimators and post compensators were put as close together as possible such that they would reflect 4 points on a circle into the collimators as shown. The mirrors redirected the light on a plane perpendicular to the pump laser, and angled the reflections to be parallel in pairs, removing the angular dependence that resulted from the cone shape of the source photons. With the light spatially separated by the mirrors the collimators were able to be placed closer to the source. Additionally the measurement devices were much easier to place, access, and manipulate. This improved the level of control, reducing loss and uncertainty.

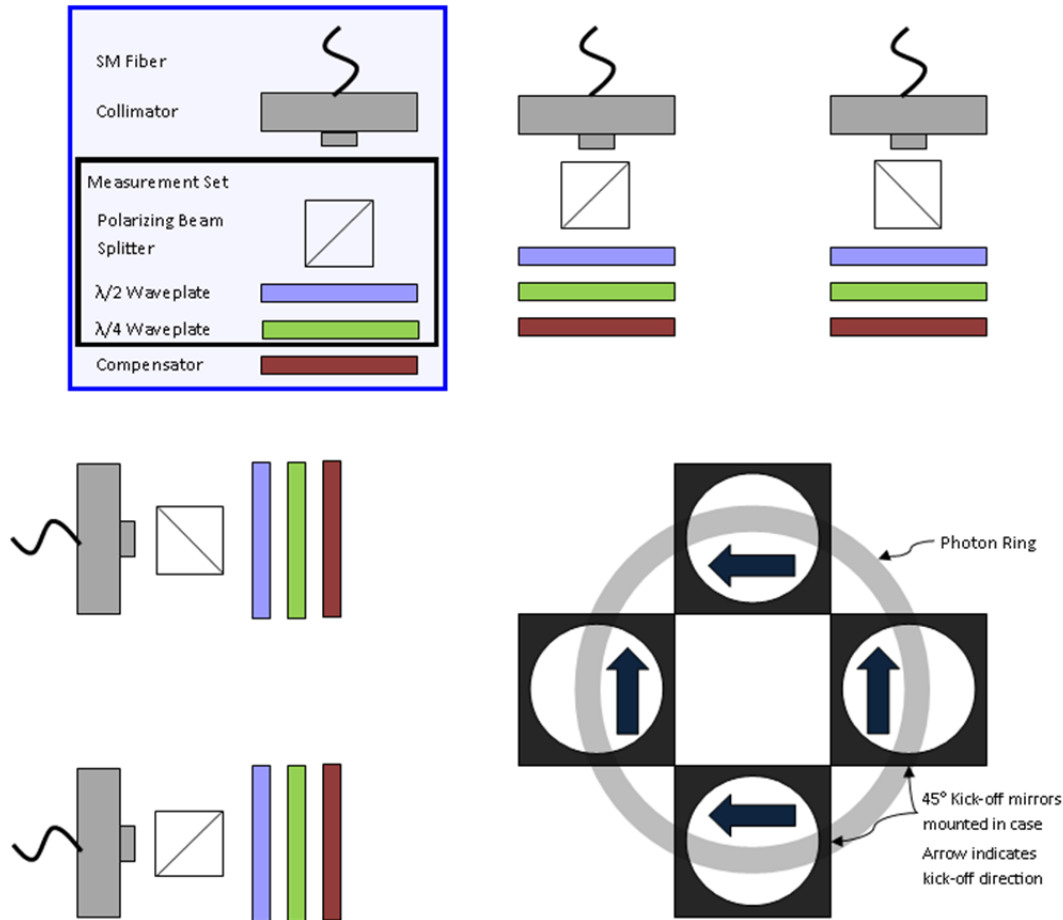


Figure 19. Entangled photon collection and measurement system.

In order to increase count rates (i.e. brightness of the source) and reduce compensation issues the SPDC crystal was switched to the α -BiBO type I crystal as used by Rangarajan [Rangarajan09] and a continuous wave laser. A CrystaLaser DL-405-025-SO, 405nm laser was used with a coherence length of $>50\text{m}$. Two independent and orthogonal pairs of photons were checked for their quality of entanglement. The measurement wave plates and PBS were placed before the collimators as shown in figure 19 ensuring photons entering the collimators had already been measured in free space. The state from the type I crystal should be $|\Psi^\pm\rangle = 1/\sqrt{2}(|HH\rangle \pm |VV\rangle)$. Table 1 shows the basis of the 16 measurements made along with the best data collected for the two different pairs; one labeled A'A the other B'B. The letter and its respective prime are used to indicate photon 1 or 2 being measured. Figure 20 shows the resulting real part of the density matrix.

Having successfully demonstrated that the two Bell pairs being produced with our collection system were of sufficient quality, the next step was to create a four cubit cluster state. This is accomplished by taking one photon from each Bell pair and entangling them with a controlled phase (CPhase) gate, as discussed in the previous section (4.1).

Table 1. Quantum tomography measurements, waveplate positions and measured concurrence.

Meas. Basis	(1) $\lambda/2$ $\theta(^{\circ})$	(1) $\lambda/4$ $\theta(^{\circ})$	(2) $\lambda/2$ $\theta(^{\circ})$	(2) $\lambda/4$ $\theta(^{\circ})$	A'A Concurrence	B'B Concurrence
$H_1 H_2$	0	0	0	0	94	129
$H_1 V_2$	0	0	45	0	4	8
$V_1 V_2$	45	0	45	0	96	118
$V_1 H_2$	45	0	0	0	5	4
$R_1 H_2$	22.5	90	0	0	51	67
$R_1 V_2$	22.5	90	45	0	49	57
$D_1 V_2$	22.5	45	45	0	37	24
$D_1 H_2$	22.5	45	0	0	65	75
$D_1 R_2$	22.5	45	22.5	90	17	110
$D_1 D_2$	22.5	45	22.5	45	106	111
$R_1 D_2$	22.5	90	22.5	45	28	103
$H_1 D_2$	0	0	22.5	45	35	48
$V_1 D_2$	45	0	22.5	45	72	75
$V_1 L_2$	45	0	22.5	0	45	43
$H_1 L_2$	0	0	22.5	0	47	86
$R_1 L_2$	22.5	90	22.5	0	109	105

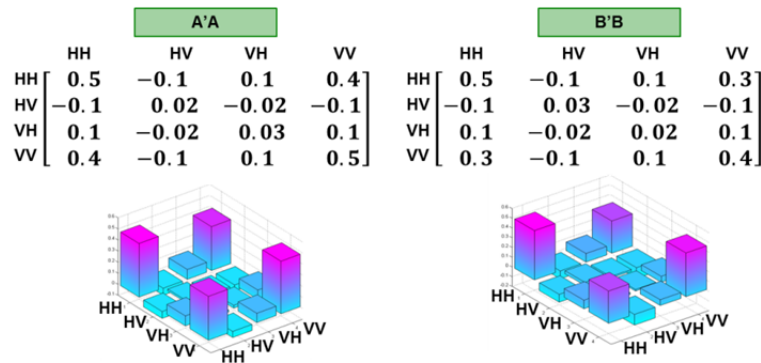


Figure 20. Density matrix of both measured pairs of photons.

In order to do this, measurements must be taken after collection and propagation through the CPhase gate, so the measurement system was removed from in front of the collimators. The post compensators remained in their original location. The fibers from two of the collimators (one from each Bell pair) were sent through a fiber polarization controller and then through the CPhase gate shown in figure 21. The photons travel through the CPhase gate in free space then propagate through the tomography measurement before being recollimated with collimators into multi-mode fiber. The multimode fiber routes the photons through a 10nm band pass filter to the detectors to remove extraneous light.

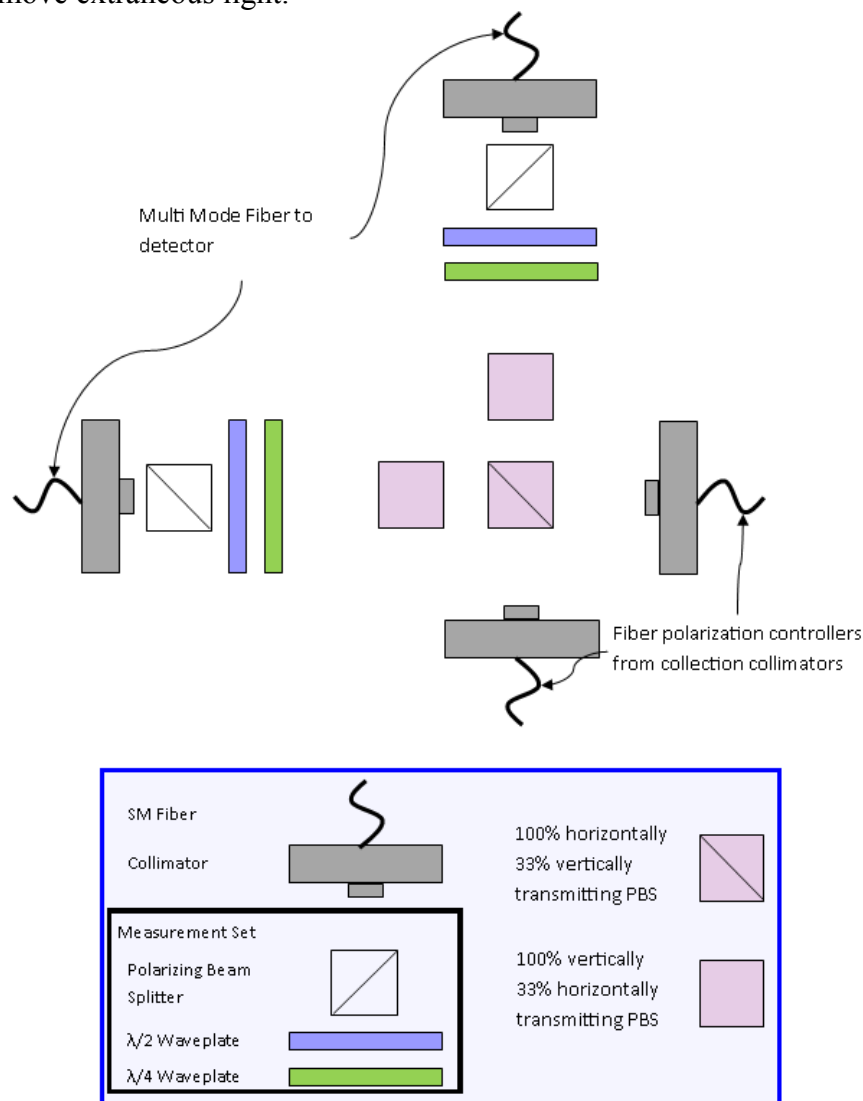


Figure 21. Controlled Phase gate system.

The other two photons from their respective Bell pairs are sent through polarization maintaining fiber, so as to match optical path length, and then in free space through a tomography measurement shown in Figure 22. The 10nm band pass filters precede the collimators in free space, and then the photons arrive at the detectors via multi-mode fiber.

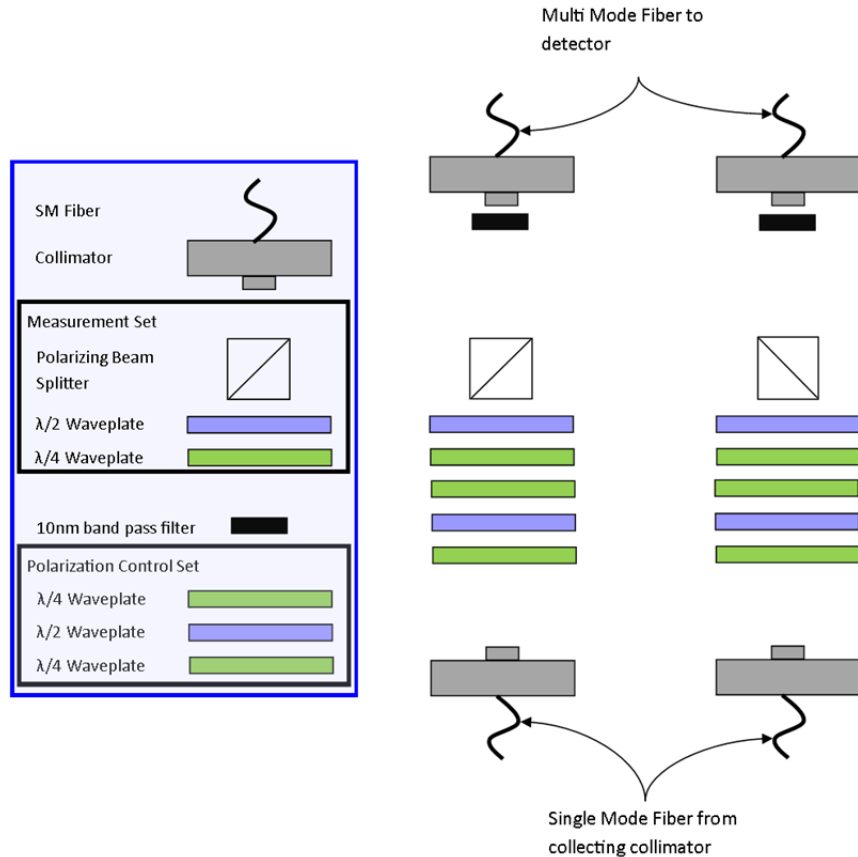


Figure 22. Free space polarization control and measurement system.

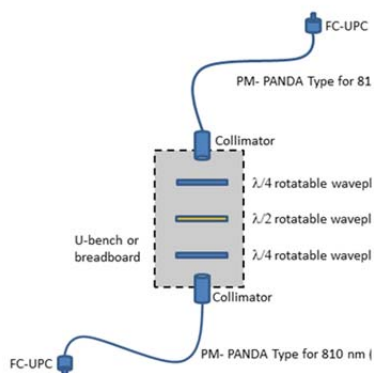
There are inherent optical losses associated with the initial free space CPhase gate configuration. To overcome these losses two hour detector integration times were required to collect a significant number of measured photons for each of the sixteen measurements. After which a tomography was performed on the output of the CPhase gate and it was apparent that the polarizations had degraded in the single mode fiber. Since the single mode fiber was not polarization maintaining, polarization rotation occurred due to changes in length and birefringence due to thermal/environmental fluctuations. The polarization controllers showed the same fluctuations as the single mode fiber, and thus did not give us enough degrees of freedom to compensate for the changes. These tests showed us the necessary changes needed to improve control of the polarization. PM fibers were installed to ensure the state was not disturbed. Additionally a polarization control set in free space was put in all four paths to correct for any residual polarization changes in the fiber. This arrangement greatly reduced the temperature dependence of the polarization; see Figure 22.

To increase the longevity of the newly revamped system an acrylic box was fabricated to create a separate environment around the crystal. This is because the BiBO and BBO crystals are very hygroscopic and when water gets into the crystal it becomes opaque and unusable. A continuous dry-air pump was installed to maintain the lowest possible humidity in the box. Additionally the polarization control and measurement wave plate systems create a lot of loss due to reflections at the multiple interfaces. We designed and ordered factory aligned and self-contained systems for each of these stages. These arrived pre-coupled to polarization maintaining single mode fibers.

When implemented these will reduce losses and speed the preparation process for any physical system needed. The construction of these components is pictured in Figure 23.

Polarization Controller

810 nm Components



Polarization Analyzer

810 nm Components

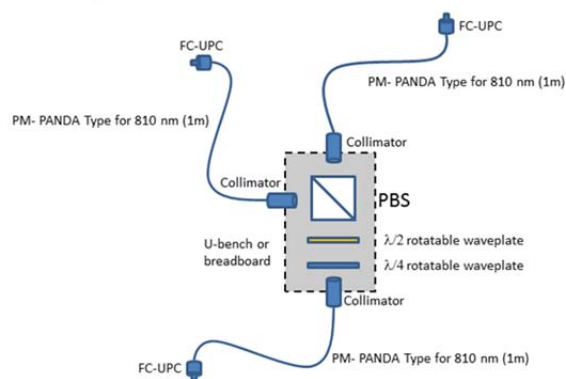


Figure 23. Professionally assembled polarization controller and measurement systems

4.3 A multi-layer three dimensional superconducting nanowire photon detector

General amplitude amplification

We now take a closer look at the minimum three layers needed to create the device, shown in Figure 24. The bottom layer 24a, consists of non-superconducting leads (red) placed on an

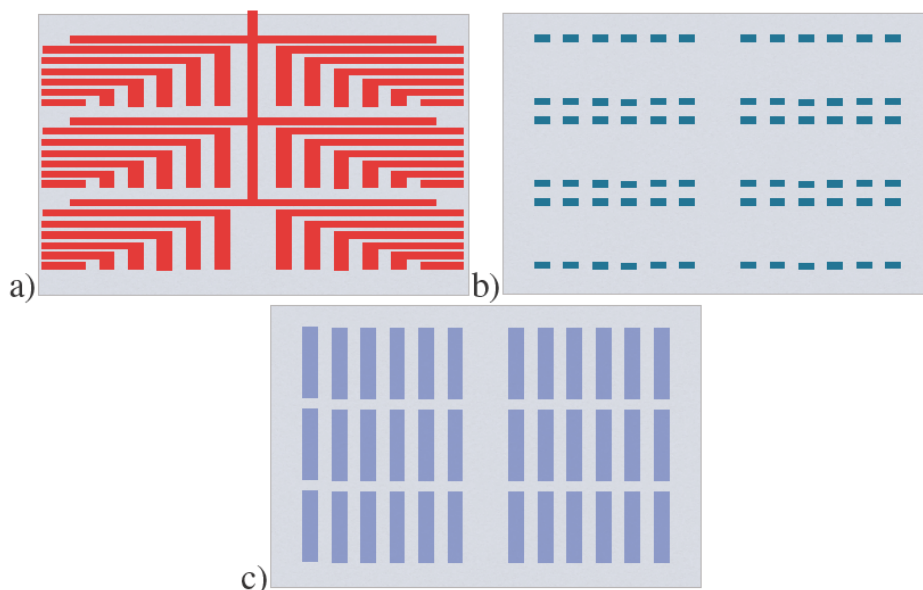


Figure 24. A plain view of the three layers in the multilayer design.

insulating substrate (gray), such as R-plane sapphire, MgO or Si. Note that there is no complete circuit on this level, so the current will be forced to move up to the next level. The optimal minimal spacing will depend on the insulating ability of the substrate to prevent leakage and cross talk, mainly between the input and output channels but also with the superconducting nanowires passing above. Over the bottom layer will be a second layer of deposited substrate

24b. This layer will then have vias, i.e. holes (green), which pass completely through it (gray) at predetermined locations so as to hit the input/output leads in the bottom layer. These vias are filled with superconducting material (in practice it may be advantageous to use non-superconducting material here, if the pixels are long enough to avoid the latching condition) thus completing the middle layer of the device. Alignment will be a very important, but not insurmountable issue, as these structures are on the scale of approximately 100nm in width and current alignment techniques can achieve results on the order of 1 nm [Anderson04]. Finally the detection layer Figure 24c, will be deposited on top of the middle layer. Alignment of the superconducting bridges with the vertical “posts” in the middle layer will be important for the overall detection efficiency [Kerman07].

The device will have significantly higher number resolution, while maintaining a useful detection area. It has several parameters which can control the reset time to avoid latching while still minimizing the rest time. An array of pixels of arbitrary number, size and shape is possible. Most of the detector will remain active after a single photon is absorbed as opposed to small number or single meander detectors which are effectively blinded by a single photon. The active area of the detector can be tuned by changing the number or the shapes of the pixels. These advantages are compelling theoretical evidence for the construction and testing of multi-layer superconducting number-resolving photon detectors.

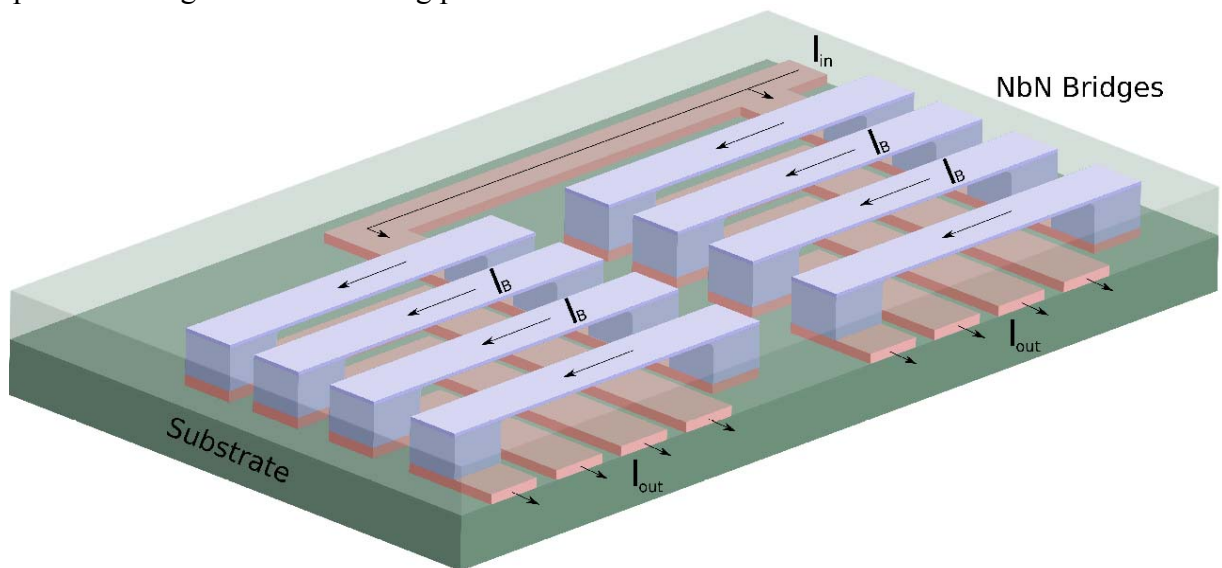


Figure 25. A toy model of a working multi-layer SNSPD. For clarity only the super-cooled part of the chip is shown. The dark green substrate and red leads are similar to the grey substrate and red leads in Figure 24a. The blue vertical posts are shown in a semi-transparent middle layer similar to Figure 24b for clarity. The blue superconducting pixels on the surface are similar to Figure 24c. The development of this design has resulted in two patents filled by the AFRL JAG officer with the U.S. patent office.

4.4 Laboratory upgrade and ongoing research in integrated waveguide quantum circuits

The Quantum Information Science Laboratory originally located in lab 18 in Bldg. 104 was relocated to a larger facility in Bldg. 3 Suite I5. The transition to the new facility allowed for the addition of 2 more optical tables, multiple work benches and equipment storage cabinets. The

facility is partitioned in two separate work areas defined by laser curtains allowing separate experiments to be conducted concurrently with lasers of class 4 or lower. During this period the Ti:Sapphire laser was upgraded from a femtosecond 1.5 W system to a femto/picosecond 3.5-4 W system. Additionally installed were both femtosecond and picosecond second harmonic generation units (SHG) were added to the system to generate powers greater than 1 W in the blue/violet regime. These additions completed the upgrade to the entangled photon generation testbed.

Further effort has been placed to reduce the footprint size of quantum gates/circuits built from bulk optical components. This added research focuses on the use of integrated optical waveguides to construct the quantum gates/circuits. The direction of the research exploits two arenas:(i) world class domestic researchers at Rome Research Site and WPAFB along with universities such as Columbia, MIT and RIT and (ii) and world class international researchers through EOARD at universities such as Bristol, Oxford and Vienna. Expanding the ongoing research in optical waveguides was a necessary step and made possible in-house with the acquisition of an optical wafer probe station. The probe station along with multiple table top probe stations will be utilized for the testing and integration of quantum photonic integrated circuits (QPIC). The entangled photons generated by the existing generation testbed are routed into the QPICs to validate the chips functionality. The acquisition of a second Ti:Sapphire laser and optical parametric oscillator (OPO) expanded the testbeds available wavelength range from the original span of 600-1000 nm to a span of 340-2500 nm. The OPO greatly increases the diversity of materials that the QPICs can be constructed from. The upgraded components have arrived and the full testbed is under construction.

4.5 Probabilistic cluster state generator (patent)

Traditional generation of a cluster state consists of an optical table several meters on each side. On this table is a high power laser system such as a pulsed Ti:Sapphire laser. The pump beam is incident on a nonlinear material such as BBO, BiBO or PPKTP etc. The photons from the pump then have a small change to undergo Spontaneous Nonlinear Parametric Down Conversion (SPDC) to create an entangled pair of photons, called signal and idler photons. Alternative means of photon generation are equally valid such as four wave mixing (FWM). To create larger linear cluster states the pump passes through multiple nonlinear materials (a cascade configuration) or is reflected back onto the original material (a multi-pass configuration). These methods can create multiple simultaneous independent pairs of qubits. To create one large cluster state the pairs are sent through (i.e. acted on by) an entangling operation. Normally the 2 qubit controlled phase gate also called the CZ gate is used. The simplest and most efficient means of implementing the general CZ gate requires 3 bulk optical asymmetric beamsplitters in a specific alignment. These operations are effectively performed in parallel with each qubit entering and exiting in its own mode. Once all the entangling operations are successfully completed the cluster state is fully constructed and an algorithm can be implemented as a sequence of single

qubit rotations and measurements on each qubit in a predetermined sequence. Thus linear cluster states are created from qubits in parallel modes rather than from sequential qubits in a single mode. This is mainly due to the spontaneous nature of single photon sources. It is impossible to predict the time between two subsequent spontaneous events.

We build upon the periodic photons source of Mower and Englund (WO2013009946 A1) to create entanglement between sequential separable qubits delivered in a single mode and create a linear cluster state of sequential qubits which is output in a single mode. Such a device is of interest in and of itself for quantum computing. Other applications include but are not limited to Measurement Based Quantum Computing (MBQC) implementation of the Deutch–Jozsa algorithm on a four qubit chain, arbitrary single qubit rotations on a four qubit chain, quantum key distribution, quantum information, quantum metrology, and quantum lithography among others.

OBJECTS AND SUMMARY OF THE INVENTION

Briefly stated, the present invention, figure 26, the Sequential Entangler or S.E., proposes to combine optical Integrated Waveguides (IW) with a periodic photon input to create linear cluster states in a single mode.

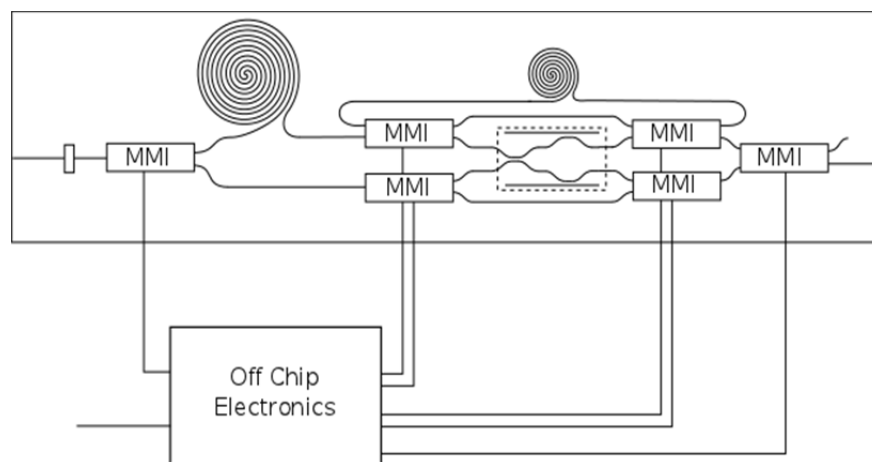


Figure 26. Sequential entangler.

We create the entanglement of sequential qubits by using a unique “loop back” architecture that delays one photon for one period T of the sequence thus allowing for two photons to be acted on by a standard entangling element. In our case we will use the simple polarization encoded CZ gate of Crespi et. al (W02012150568A1). One photon (now entangled so which cannot be determined) is then released and the second is looped back to coincide with the arrival of the next photon and so on. This will probabilistically produce a linear cluster state. We say probabilistically as the CZ gate succeeds only 1 time in 9. Thus the longer a desired cluster state is the less likely it is to be created in any one attempt. This is a result of the entangling operation and not the S.E. per say as no photonic entangling operation can be performed with unit success.

The S.E. will create a cluster state numerically identical to the industry standard parallel method but arranges the qubits as a periodic sequence (with a constant period T) in a single optical mode. Any two qubit entangling operation can be used in place of the CZ however such gates may produce different cluster states.

A significant improvement on cluster state generation is possible with on demand photon sources. Such a source emits a single photon or pair of photons at a specified time, eliminating the need for probabilistic photon generation. No such device currently exists in the state of the art. As an approximation to an on demand source the “photon gun” was proposed by Mower Englund (WO2013009946 A1). This device remains probabilistic but has a relatively high probability of producing a single photon at a predetermined time and is in fact intended to be periodic. In other words it will with relatively high probability emit a single photon after every time T . The photon gun creates pairs of photons via probabilistic means from time 0 to $T-1$ and then detects (and thus destroys) the presence of one of those photons to herald the presence of the remaining photon. This heralded photon is then delayed in a variable circuit until time T . The device is nearly periodic because the probability of at least one pair being generated before time $T-1$ is close to 1. Thus the photon gun sacrifices repetition rate in order to maximize the photon production probability. Our device can be trivially modified to incorporate a fully on demand source should one become available. Modifications to the device may either decrease the complexity or increase the functionality. Moving the delay line from the first path to the bottom path can create a symmetric device and also reduce the long integrated waveguides which can reduce loss, as shown in figure 27.

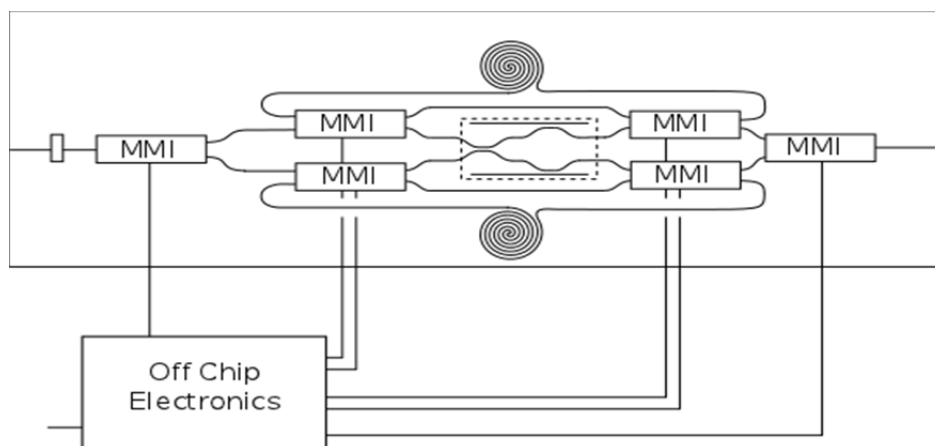


Figure 27. Symmetric sequential entangler.

A second modification is to increase the number of delays as shown in figure 28. The incorporation of the additional switchable delay allows entangling photons in a two dimensional cluster state as opposed to just a linear chain.

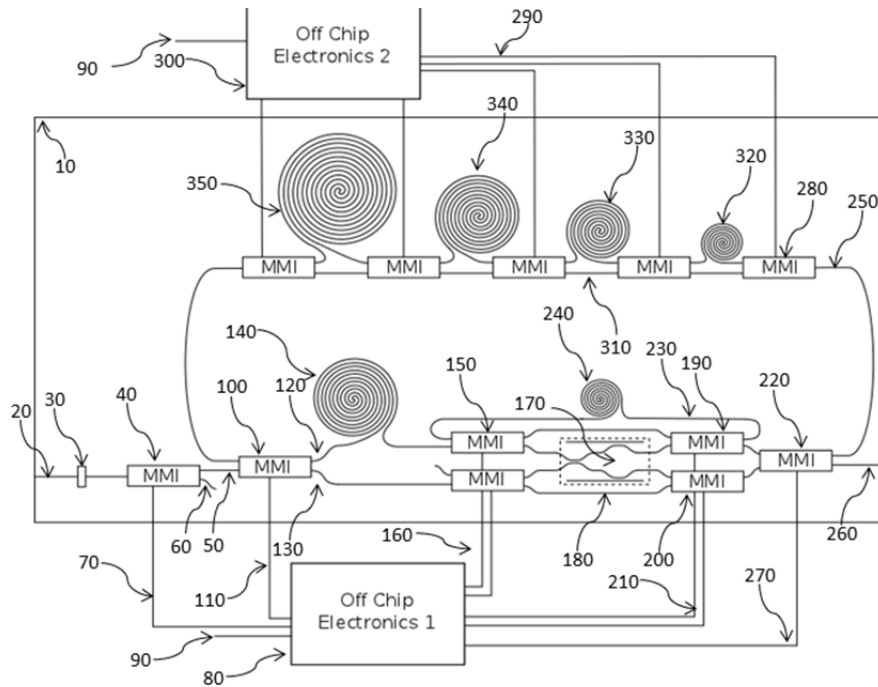


Figure 28. Two dimensional cluster state generator.

Importantly, one advantage of on demand, or probabilistically close to on demand, photon sources is the ability to avoid having to create an arbitrarily large initial cluster state for MBQC as first envisioned by Breigel and Raussendorf. Rather it is possible to create a continuously flowing cluster state in which new qubits are periodically created and added to the current cluster state by entanglement while at the same time other qubits are removed from the cluster state by projective measurements. If the entanglement occurs on one side of the cluster, the measurement occurs on the opposite side and the rate of adding photons is the same as the rate of removing photons, then the cluster state can be said to “flow” across the device. We create such a flowing cluster state by creating photons and entanglement on one side of our integrated waveguide chip measuring the photons on the other side, in an alternate formulation of our device.

Briefly stated, the present invention proposes to combine multiple “photon guns” with tunable integrated waveguide (IW) circuitry and entangling operations to create a periodic probabilistic 2D photonic cluster state, with the additional feature of having independent control (on/off) of each of the entangling operations (i.e. internal interconnections). Given that the number of modes is large enough, the cluster states created by this device will be able to perform universal computations. In addition, the control of the internal interconnections allows for the construction of arbitrarily shaped and interconnected cluster states as well as multiple (smaller) cluster states from a single device. These controls will be simple electrical inputs and can be switched at high speed. The resulting device attempts to produce a desired cluster state after every time T_{CS} . We call this device a Periodic Cluster State Generator (PCSG), as shown in Figure 29.

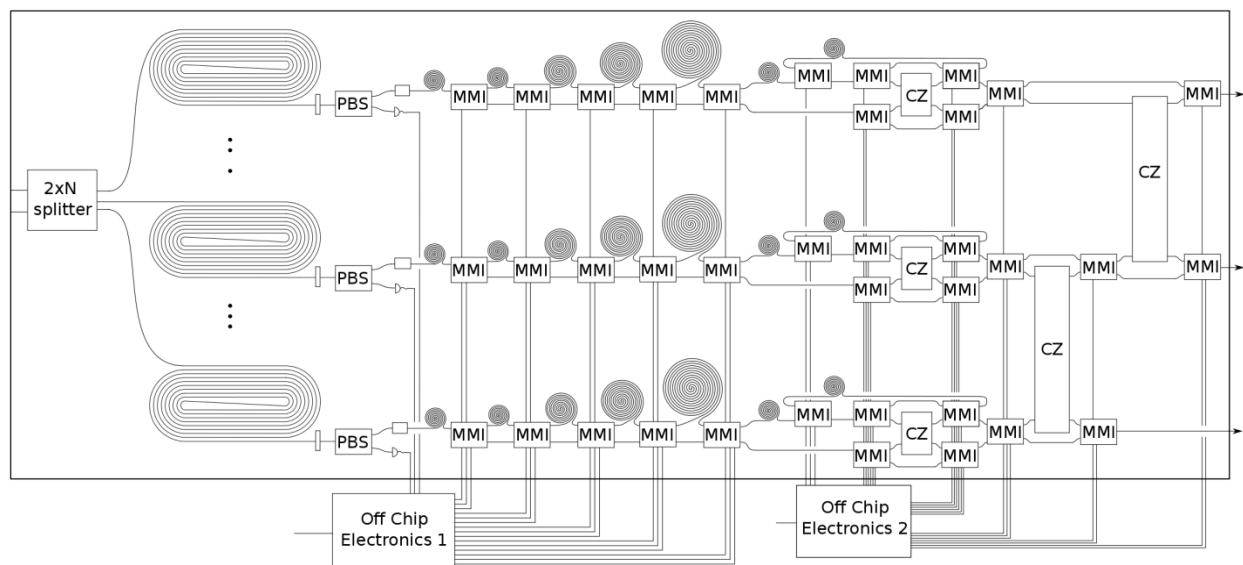


Figure 29. Probabilistic cluster state generator.

A preferred embodiment of the present invention (PCSG) consists of a monolithic Integrated Waveguide (IW) chip consisting of two fundamental operations, photon generation and controllable entanglement. To produce the cluster state at high speeds while minimizing the waveguide length the waveguide chip must be capable of rapid switching. Electro-optical materials such as Lithium Niobate (LiNbO_3), as opposed to slower thermal switching materials, are preferred. We note the device will work in materials with slow switching but will have longer delay lines and may need to be larger itself to compensate. The waveguides fabricated within the waveguide chip must be polarization maintaining (PM) waveguides as we will encode the qubits in the photons polarization.

Our preferred implementation generates photons on the principle of FWM as has been demonstrated in waveguides previously. Our device consists of two input modes. One for each of the two “waves” needed to pump the device. These modes are incident on an integrated two by N splitter based on evanescent coupling, where N is the number of guns in the device. This number, N, has no theoretical upper bound. This element separates the pumps evenly into the n modes in which the 4 wave mixing takes place. Such a device simplifies the problem of maintaining synchronization between modes that is difficult if each mode is individually pumped. The photons created will have orthogonal polarizations which can be set to horizontal and vertical. In order to increase the count rate for this probabilistic process we create large equal length meanders in each wave guide that increase the interaction time. We note that any device or method that creates photon pairs could be used with trivial modifications to the circuit design.

In our preferred embodiment the photons in the waveguides are then incident on hyper-spectral filters which block the propagation of both pumps. The position of the spectral filtering is not critical to the design and can be performed anywhere in the circuit after the FWM has occurred

including at the end of the circuit. To use non-degenerate FWM this filter would be replaced with a standard wave division multiplexer (WDM) which dumps the pump wavelengths into a mode that exits the IW chip or is bulk terminated in the chip, while allowing the signal and idler photons to propagate. Any such device that separates the pump photons from the desired photons is equally valid to this invention.

In our preferred embodiment the signal and idler photons travel along another section of waveguide of arbitrary size and shape and are incident on a Multi-Mode Interferometer (MMI). This MMI acts as a polarization beam splitter and separates the horizontal and vertical photons into two separate modes (any device that accomplishes this goal is equally valid in our device). One photon (which polarization is used is not relevant) is detected and therefore destroyed. This is done in order to herald the existence of the second photon in the propagating mode. The type of device used to detect the presence of this photon is not relevant to the device in question and can be performed either on the IW or off chip. Our preferred embodiment of the PCSG will use integrated single photon detectors such as but not limited to superconducting nanowire single photon detectors or transition edge sensors. Such detectors can be fabricated directly into the IW itself but require $<10\text{K}$ (kelvin) temperatures to operate. Thus integrating the detector requires super cooling the entire chip. As the efficiency of this detector is critical to the device's operation the most efficient available detector is desired. We note that the device can be designed to operate with low efficiency detectors and a given pump rate by increasing the number of delay segments (defined below) at the cost of reducing the repetition rate. As the previous section the PCSG creates photons with known orthogonal polarizations and as all waveguides are polarization maintaining it is a trivial process to rotate the propagating photons to the $H+V$, or the $|+\rangle$ state (ignoring normalization) by industry standard devices. This can be done at any point prior to the entangling operations.

The photon generation method and heralding detection method of the PCSG is relatively arbitrary in that the PCSG can be trivially modified to accommodate different designs. Regardless of the photon generation and detection method the next step of the "photon gun" is critical. See Mower and Englund (WO2013009946 A1). Each pump pulse has a non-unitary (i.e. less than perfect) chance to create a photon pair and the detectors have a less than perfect chance of detecting one of these photons. Thus each pulse will not create a photon, in even the most ideal case. Different techniques can be used to improve these probabilities but cannot be made perfect with the current state of the art technology. Thus the "photon gun" is not periodic but probabilistic. The PCSG is also probabilistic as it generates photons with period T and success probability approaching one. The critical time bucket T consists of N time bins t such that each bin is synchronized with one and only one pulse from the pump ($T=Mt$). The number of time bins required M is determined such that with very high probability at least one photon pair is produced and heralded in each time bucket T . This is dependent on a large number of factors but can be determined by standard methods.

The heralded but undetected photon, now in the $|+\rangle$ state, is then delayed in variable delay lines until it is emitted at time T or $T+1$. This is achieved through a series of identical delay lines which the heralded photon can be diverted into by rapidly tunable MMIs. The switches that control the photon path and therefor the delay time are controlled by off chip electronics. This device records the detection time of the heralded photon and compares it to the clock time. Thus the off chip electronics can determine in which time bin t_p the photon pair was generated and the needed delay time $(T-t_p)$. Then the electronic device sets the output ports for the tunable MMIs (i.e. switch directions) to implement the required delay. In the preferred embodiment this is done with industry standard electro optical control. While this calculation and reconfiguring is taking place the photon is stored in an arbitrarily shaped waveguide. The length of this first delay, Delay A, is determined by the maximum time required to herald and successfully reconfigure the device and in general will not be the same (most likely longer) then the time bin delay lines. These steps happen simultaneously in each parallel mode. The result of the first section of the PCSG is a periodic (in time) sequence of synchronized arrays of N photons. In other words this first section of PCSG creates an un-entangled flowing grid of photons of size N and arbitrary length. The probabilistic nature of the PCSG means there will be some holes in the grid where no photon was successfully produced or a photon was lost. We note that the photon gun section of the PCSG could be trivially replaced with an array of non-probabilistic on demand single photon sources. Such sources could be periodically triggered to release a known photon state and reproduce the output of the photon guns described above without changing the scope or spirit of this invention.

The photons are then guided to the second part of the PCSG that performs the controllable entanglement on the photon grid. In our preferred embodiment these two sections are both on the same monolith IW chip. But fabrication may be simpler if the device is fabricated on two (or more) chips. The monolithic WG chip has the advantage of compactness, stability and no losses due to coupling chips into and out of fibers.

The second section of the Monolithic IW chip in our preferred implementation creates the horizontal entanglement between sequential qubits. This is an application of the Sequential Entangler of Smith and Fanto, and in fact requires an array of Sequential Entanglers. In our preferred implementation the tunable MMI at the end of the “photon gun” serves a double purpose. In addition to assisting in controlling the delay time it also transfers the output photons to one of two modes. In our preferred implementation the MMI begins by putting the first photon in the “upper” mode. By which we mean that the incident photon exits the MMI in the “upper” mode in relation to the figures bellow. The device can be trivially modified to use either output. Any device that is capable of deterministically switching the output mode of a photon is a viable alternative which doesn’t affect the function, scope or spirit of the device. The first photon, arriving in each parallel mode after time T , is then delayed in a waveguide delay line, Delay B, for exactly one period of time T . The MMI is then switched to the “lower” mode before the arrival of the second photon at time $2T$ by an off chip electric circuit. The maximum repetition

rate of the PCSG is thus limited by the minimum switching time of the MMIs or any reconfigurable device that replaces it.

The two separate $|+\rangle$ state photons, one in the “upper” mode and one in the “lower” mode, are then each incident on another MMI. One output mode of each of this pair of MMIs feeds into the entangling operation. The other leg of each MMI is routed around the entangling operation in a “bypass” mode. The length of the bypass mode is designed such that it is the same as that in the entangling operation. The routing operation is implemented in the same manner as previous MMIs and is controlled by off chip electronics. In our preferred implementation the entangling operation is the integrated waveguide CZ gate of Crespi et. al (W02012150568A1). The gate consists of several static evanescent couplers. The current state of the art of entangling operations has many implementations of this gate and numerous other gates. Any of these gates may be used to create trivial variations of the PCSG for custom purposes. The CZ gate has a success probability of $1/9$ per instance. Therefore long chains are increasingly unlikely to be successfully created. Thus a high repetition rate is desirable, such that many attempts can be made in a short time. Also any improvement in the success rate of the entangling gate is desirable and represents a trivial alteration to the PCSG that doesn’t change the function, scope or spirit of the invention.

The modes from the entangling operation are then merged with the “by pass” modes by additional MMIs. One photon is allowed to propagate while the other is “looped back” into the device to such that it can be entangled with the next photon in the sequence. Rapid switching gives the capability to “add” or “remove” horizontal entanglement in between any sequential qubits in a cluster state.

The third photon produced in each mode reaches the sequential entangler while one photon from the first pair is stored in a delay line, Delay C. The length of this delay line is such that these two photons will be synchronized upon reaching the paired MMIs before the CZ gate. The third and all subsequent photons are routed into the “down” path. Which photon is “looped back” after the CZ gate cannot be determined due to the nature of entanglement. Therefore either mode may be fabricated with the “loop back” feature or equivalently either formulation of the Sequential Entangler.

The photons then exit the parallel set of sequential entanglers in the PCSG and enter the final section of the device. This section implements the vertical entangling gates between synchronized qubits in different modes. This section consists of a cascade of industry standard entangling operations. In our preferred implementation these entangling operations are again the CZ gate of Crespi et. al (W02012150568A1). Similar to the last section any entangling operation can be trivially used in place of any or all of the CZ gates for custom purposes. The CZ gates are placed such that each mode interacts with its neighbors, this condition can be relaxed or altered for specific purposes without materially changing the invention. The photons are incident on MMIs which, similar to above, have one output routed to the CZ gate and one output routed to a “bypass” line. The MMI are controlled by off chip electronics and rapid switching, i.e. the rapid

switching rate allows for controlling the placement of vertical entanglement between specific qubits (i.e photons). Delay lines may be used to maintain synchronization of all modes.

Combining the effect of the controllable MMIs allows for any size and shape cluster state to be created, within the following limits. The square shape of the grid remains (i.e.), the maximum size of the grid N is set by the fabrication of the device and in our preferred embodiment only nearest neighbor interactions are used. Any arbitrary number and shape of nearest neighbor connections are then possible by preforming rapid switching of the various paired MMIs which control the bypass lines around each individual entangling operation. If all of the CZ operations are used the resulting output (in theory) would be an arbitrarily long flowing grid of entangled qubits, N rows tall. In practice the probabilistic nature of the PCSG means that attempting to make larger and larger cluster states and states with more entangling interactions becomes increasingly unlikely. This is also true of any state of the art device and implementation. The high repetition rate possible with the monolithic IW PCSG device proposed here allows for many, many attempts to be made in comparatively short time frames (i.e. a high repetition rate) with excellent stability and limited coupling losses. Thus relatively large and complicated cluster states can be made with the PCSG that would be impractical with other setups.

An alternate formulation of the PCSG for the purpose of MBQC is provided below. Here rather than outputting the cluster state from the chip addition hardware is fabricated such that quantum enhanced computation can be performed. Such an alternate formulation can be considered a quantum computer on a single chip. The size of the computation is limited only by the number of output modes the device is fabricated with. A two dimensional square nearest neighbor cluster state has been shown to be a universal resource for MBQC thus we can say our quantum computer is universal. We note that arbitrarily large calculations will require arbitrarily long cluster states and due to the non-deterministic generation of cluster states in the PCSG such arbitrarily large cluster states will take an arbitrarily long time to successfully generate.

We also note that in our preferred implementation the off chip electronics are broken into three devices each serving its own purpose. “Off chip electronics 1” detects/heralds the presence of photons and reconfigures the delay line circuit. “Off chip electronics 2” controls the placement of the entanglement in the cluster state. “Off chip electronics 3” for our alternate formulation implements the MBQC algorithm of single qubit rotations and detection events. These three operations can be combined into a single classical device without altering the details of their operation. Indeed combining the off chip electronic into a single circuit will make synchronization simpler and allow for further scalability.

4.6 Theory/experimental requirements of imperfect two-qubit linear optical photonic gates

The optimization method we have developed maximizes the success probability S for a given target transformation A^{Tar} , for given ancilla resources, and for a given fidelity level $F \leq 1$. This is mathematically equivalent to unconstrained maximization of the function $S + F/\epsilon$ in the space of all matrices U , where $1/\epsilon$ is a Lagrange multiplier. Here $\epsilon \rightarrow 0^+$ corresponds to maximizing the success probability while requiring perfect fidelity ($F = 1$). As ϵ is increased, the maximum of S

+ F/ϵ yields linear optics transformations that maximize the success S as a function of the fidelity F . Given one transformation U that (locally or globally) maximizes success S for a given fidelity F , ϵ may be continuously varied to obtain a one-parameter family of optimal transformations, tracing out a curve in success-fidelity space. Note that in general the members of these families need not be all unitary, however for some gates of interest, including the CZ gate, all members of the family are unitary. Figure 20 shows optimal results for the CZ gate. Here each point corresponds to a unique unitary mode transformation U . As previously reported we find an interesting feature of these unitary matrices. The optimal solution with fidelity $F = 1$ was found by Knill to have a surprising form [Knill02], which we have dubbed the “Knill Form” [Uskov09], where one mode of each qubit is non-interacting, e.g., in the CZ case U acts as the identity on modes 1 and 3 (or equivalently 1&4, 2&3, or 2&4). This form has been found to hold for the CZ gate and for the TS Toffoli Sign gate (CNOT and Toffoli respectively are equivalent to these up to local rotations).

We now propose an experiment that will test the results shown in Figure 30. Reck et al. [Reck94] have shown that any discrete $N \times N$ unitary transformation U can be implemented as a multi-port device consisting only of variable transmittance beamsplitters and phase shifters [Reck94]. Their method is a decomposition in which each unitary matrix element below the diagonal is transformed into zero by a 2×2 rotation matrix embedded in an $N \times N$ matrix which is otherwise equal to the identity. For example, the 2×2 rotation acting on modes N and $N-1$, which eliminates the element $U_{N,N-1}$, takes the form $T_{N,N-1}$ shown in Figure 30.

$$T_{N,N-1} = \begin{pmatrix} 1 & \cdots & \cdots & 0 \\ \vdots & \ddots & e^{i\phi} \sin(\omega) & e^{i\phi} \sin(\omega) \\ 0 & \cdots & e^{i\phi} \sin(\omega) & e^{i\phi} \sin(\omega) \end{pmatrix}$$

Figure 30. Rotation matrix for modes $N-1$ and N .

The method is recursive and requires one iteration for each pair of modes. Finally, we obtain $U(N)T_{N,N-1}T_{N,N-2} \dots T_{2,1}D = I$ where D is a diagonal matrix of phases. The desired transformation U is then decomposable as $U(N) = D^{-1}T_{2,1}^{-1}T_{3,1}^{-1} \dots T_{N,N-1}^{-1}$. Physically, each $N \times N$ transformation $T_{i,j}^{-1}$ is implemented as a variable transmittance beamsplitter with a phase plate on one input mode, while D^{-1} corresponds physically to a phase shift on each output mode [Reck94]. Thus a generic two-qubit operation, which needs at least $N = 7$ modes ($N_c = 4$ computational modes and $N_a = 3$ ancillas) requires a minimum of 21 beamsplitters and 28 phase shifters. A controlled unitary gate ($N = N_c + N_a = 4 + 2 = 6$) requires at least 15 beamsplitters and 21 phase shifters. If unitary dilation is required (as is often the case) the number of optical elements increases rapidly. However our experiment does not require unitary dilation and furthermore as noted by Reck et al., if an element of the unitary matrix is already zero, then no transformation is required. The element is skipped.

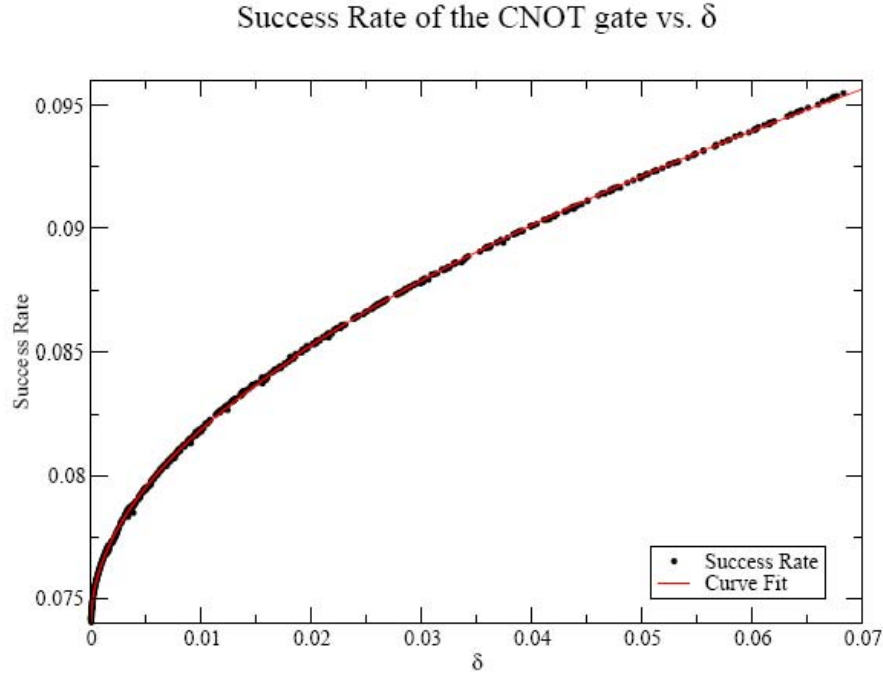


Figure 31. Improved success rates for compromised δ .

Here we return to the “Knill Form,” where in the case of CZ we find that nine of the elements below the diagonal are already zero. Therefore the unitary transform can be implemented with only six beamsplitters and 10 phase shifters. We can perform this decomposition for each data point in Figure 31, and find the rotation angles $\omega_{i,j}$ and phases $\phi_{i,j}$ in each case. Surprisingly we find numerically that all of the phase shifts, $\phi_{i,j}$, are constant along the entire length of the curve in Figure 31. Therefore only the six beamsplitter rotation angles $\omega_{i,j}$ out of a total of 36 possible variables need to be modified to vary, making the experiment much more physically realizable. To be specific, the transformation only requires beamsplitters acting on the following mode pairs: $(i, j) = (6, 5); (6, 4); (6, 2); (5, 4); (5, 2); (4, 2)$. Figure 32 shows that the six beamsplitter rotation angles change smoothly with δ . Implementing such rotations and constant phase shifters will recreate the unitary matrices from Figure 31.

This system lends itself to being implemented with 2x2 Mach-Zehnder interferometers (MZI) in place of standard beamsplitters. The transmittance (Figure 32) of the MZI is controlled dynamically by adjusting the phase difference, without having to alter the physical system. These interferometers have already been put on optical chips by Thompson et al. [Sohma94] among others. Indeed, significantly larger electro-optical matrix switches have been proposed and built

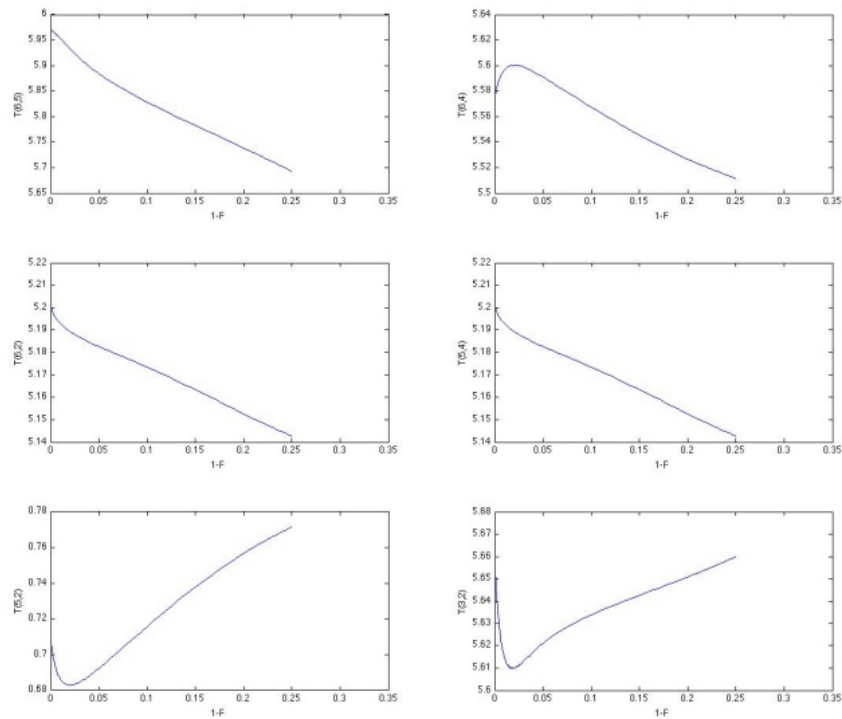


Figure 32. Beamsplitter transmissivity

for broadband optical communication networks [Sohma94, Drever83]. Figure 33 shows a multiport device that mixes seven input/output modes (thin lines) using 2x2 variable transmittance beamsplitters (rectangles), each of which has a phase shifter on one of its input modes (ellipses). An additional phase shifter is placed on each device output mode. The thick line is a simple mirror. J. L. O'Brien recently proposed a similar 7x7 single-chip MZI-based device made from lithium niobate waveguides [Sohma94]. The intended purpose of this chip was to be able to perform any two-qubit unitary operation, i.e. any transformation in $SU(4)$. However, such a device would also be capable of performing the experiment described above.

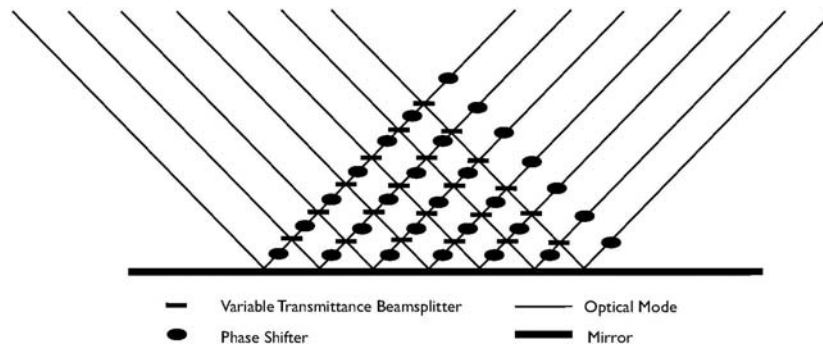


Figure 33. General multiport device schematic.

4.7 Nonlocality, entanglement witnesses and supra-correlations

No Signaling (NS) Correlations: 2-Qubits

Following Acin *et al.* [Acin10] we define an n -partite probability distribution $P(a_1, \dots, a_n | x_1, \dots, x_n)$ as being NS if and only if there exists local quantum measurements $M_{a_i}^{x_i}$ and a Hermitian operator O of unit trace such that (14) holds. It is important to note that O need not produce positive probabilities for other measurements outside this set. Acin *et al.* [Acin10] give a prescription for the formal construction of O given the set of measurements $M_{a_i}^{x_i}$. In the following we present an explicit construction for O for the case of $n=2$ qubits ($r=2$ outputs, i.e. $a, b = \{0,1\}$) and arbitrary number m of measurement inputs ($x, y = \{0,1, \dots, m-1\}$). Later, we extend this to the case of $n=3$ for qubits.

As stated in Section 3.4, without loss of generality we can take the local Hermitian measurement operators to be the projection operators onto “spin-component” a in the “direction” x , $M_a^x = \Pi_a^x = |a\rangle_x \langle a|$. For each x , the completeness of the measurement operators give $\sum_{a=0}^{r-1} M_a^x \equiv I_{r \times r}$ where $I_{r \times r} \equiv I$ is the $r \times r$ identity matrix. This allows us to write the $a=r-I$ measurement operator as $M_{a=r-1}^x \equiv I_{r \times r} - \sum_{a=0}^{r-2} M_a^x$. One defines the (tilde) Hermitian matrices \tilde{M}_a^x dual to M_a^x through the inner product $\text{Tr}[M_a^x \tilde{M}_{a'}^{x'}] = \delta_{x,x'} \delta_{a,a'}$. For the bipartite case $n=2$, with in general m measurement settings with r measurement outcomes, one has

$$O = \sum_{a,b=0}^{r-2} \sum_{x,y=0}^{m-1} P(a,b | x, y) \tilde{M}_a^x \otimes \tilde{M}_b^y + \sum_{a=0}^{r-2} \sum_{x=0}^{m-1} P(a | x) \tilde{M}_a^x \otimes \tilde{I} + \sum_{b=0}^{r-2} \sum_{y=0}^{m-1} P(b | y) \tilde{I} \otimes \tilde{M}_b^y + \tilde{I} \otimes \tilde{I}, \quad (24)$$

where \tilde{I} is the tilde matrix dual to the $r \times r$ identity matrix I , with the additional orthogonality conditions defined by $\text{Tr}[I \tilde{I}] = \text{Tr}[\tilde{I}] = 1$, $\text{Tr}[M_a^x \tilde{I}] = 0$, and $\text{Tr}[I \tilde{M}_{a'}^{x'}] = \text{Tr}[\tilde{M}_{a'}^{x'}] = 0$. The conditions

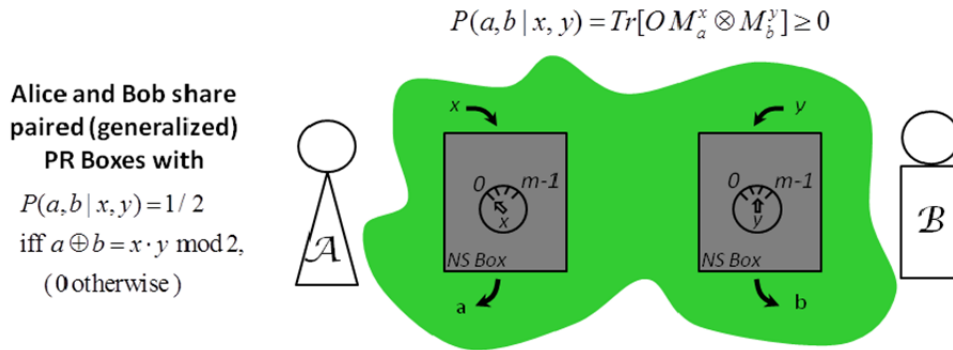


Figure 34. PR Box shared between Alice and Bob.

ensure that O is Hermitian, $\text{Tr}[O]=1$ and probabilities are given by the trace formulas $P(a, b | x, y) = \text{Tr}[O M_a^x \otimes M_b^y]$, $P(a | x) = \text{Tr}[O M_a^x \otimes I]$ and $P(b | y) = \text{Tr}[O I \otimes M_b^y]$. This is illustrated in

Figure 34 where Alice and Bob share PR correlations by means of, what are termed in the literature, a pair of *PR boxes* (or NS {non-signaling} boxes).

In the following we specialize to the case of qubits ($r=2$, $a,b = \{0,1\}$) with arbitrary number m of measurement inputs ($x,y = \{0,1,\dots,m-1\}$). In this case the measurement operators $M_{a=0}^x$ are given as projection operators for “spin-up” along the directions $x \rightarrow \vec{m}_x$ on the Bloch sphere. The $M_{a=0}^x$ are just density matrices on the Bloch sphere written as

$$M_{a=0}^x = |0\rangle_x \langle 0| = 1/2(I + \vec{m}_x \cdot \vec{\sigma}), \quad \vec{m}_x = m_x(\sin \theta_x \cos \phi_x, \sin \theta_x \sin \phi_x, \cos \theta_x) \quad (25)$$

$$|\vec{m}_x| \leq 1, \text{ (density matrix on Bloch Sphere),}$$

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ is the vector of single qubit Pauli matrices. Although not required for the case of qubits, the projection onto “spin-down” along x is given by $M_{a=1}^x = |1\rangle_x \langle 1| = 1/2(I - \vec{m}_x \cdot \vec{\sigma}) = I - M_{a=0}^x$, with I the 2×2 identity matrix. Equation (17) now simplifies to the form

$$O = \sum_{x,y=0}^{m-1} P(a=0, b=0 | x, y) \tilde{M}_0^x \otimes \tilde{M}_0^y + \sum_{x=0}^{m-1} P(a=0 | x) \tilde{M}_0^x \otimes \tilde{I} + \sum_{y=0}^{m-1} P(b=0 | y) \tilde{I} \otimes \tilde{M}_0^y + \tilde{I} \otimes \tilde{I}. \quad (26)$$

We simplify the notation by defining $\{I, M_{a=0}^x; x=0, \dots, m-1\} \equiv \{M_{-1} \equiv I, \{M_{i \geq 0}\} = \{M_{-1}, M_0, M_1, \dots\}\} = \{M_{\alpha=\{-1, i \geq 0\}}\}$ (a set of $m+1$ linear independent matrices) with duals $\{\tilde{M}_{\beta=\{-1, j \geq 0\}}\} \equiv \{\tilde{M}_{-1} \equiv \tilde{I}, \tilde{M}_0, \tilde{M}_1, \dots\}$ satisfying the trace orthogonality conditions $\text{Tr}[M_\alpha \tilde{M}_\beta] = \delta_{\alpha,\beta}$, and similarly for $\{I, \{M_{j \geq 0}^y\}\} \rightarrow \{N_{\beta=\{-1, j \geq 0\}}\}$. We therefore write (26) as

$$O = \sum_{i,j=0}^{m-1} P_{i,j}^{0,0} \tilde{M}_i \otimes \tilde{N}_j + \sum_{i=0}^{m-1} P_i^{0,\bullet} \tilde{M}_i \otimes \tilde{I} + \sum_{j=0}^{m-1} P_j^{\bullet,0} \tilde{I} \otimes \tilde{N}_j + \tilde{I} \otimes \tilde{I}, \quad (27)$$

using the abbreviations $P_{i,j}^{0,0} = P(a=0, b=0 | x=i, y=j)$, $P_i^{0,\bullet} = P(a=0 | x=i)$ and $P_j^{\bullet,0} = P(b=0 | y=j)$. For the measurement matrices $M_{-1} = I \equiv I_{2 \times 2}$, and $M_{i \geq 0} = 1/2(I + \vec{m}_i \cdot \vec{\sigma})$, $|\vec{m}_i| \leq 1$, the dual matrices are given explicitly by $\tilde{M}_{-1} \equiv \tilde{I} = 1/2(I - \sum_{i \geq 0} \vec{m}_i \cdot \vec{\sigma}) \equiv 1/2(I - \vec{m} \cdot \vec{\sigma})$, and $\tilde{M}_i = \vec{m}_i \cdot \vec{\sigma}$ where $\vec{m}_i \cdot \vec{m}_j = \delta_{i,j}$, $|\vec{m}_i| \geq 1$, with the orthogonality relations $\text{Tr}[\tilde{I}] = 1$, $\text{Tr}[\tilde{M}_j] = 0$, $\text{Tr}[M_i \tilde{I}] = 0$, and $\text{Tr}[M_i \tilde{M}_j] = \delta_{ij}$. Using the relationship $\text{Tr}[X \otimes Y] = \text{Tr}[X] \text{Tr}[Y]$ it is straightforward to verify that $\text{Tr}[O] = 1$ and, for example, $P_{i,j}^{0,0} = \text{Tr}[O M_i \otimes N_j]$ which picks out the term $\tilde{M}_i \otimes \tilde{N}_j$ in (20). Other probabilities are obtained for example as $P_{i,j}^{0,1} = \text{Tr}[O M_i \otimes (I - N_j)] = \text{Tr}[O M_i \otimes I] - \text{Tr}[O M_i \otimes N_j] = P_i^{0,\bullet} - P_{i,j}^{0,0} = \sum_{b=\{0,1\}} P_{i,j}^{0,b} - P_{i,j}^{0,0} = P_{i,j}^{0,1} = P(a=0, b=1 | x=i, y=j)$. Substituting the explicit expressions for the dual matrices into (27) yields the general expression for O in terms of products of Pauli matrices

$$O = \frac{1}{4} \left[\sum_{i,j=0}^{m-1} (4P_{i,j}^{0,0} - 2(P_i^{0,\bullet} + P_j^{\bullet,0}) + 1) (\vec{m}_i \cdot \vec{\sigma}) \otimes (\vec{n}_j \cdot \vec{\sigma}) \right. \\ \left. + \sum_{i=0}^{m-1} (2P_i^{0,\bullet} - 1) (\vec{m}_i \cdot \vec{\sigma}) \otimes I + \sum_{j=0}^{m-1} (2P_j^{\bullet,0} - 1) I \otimes (\vec{n}_j \cdot \vec{\sigma}) + I \otimes I \right]. \quad (28)$$

Specializing to the PR correlations in (10) given by $P(a, b | x = i, y = j) = 1/2 \delta_{a \oplus b, i \cdot j \bmod 2} \Rightarrow P_{i,j}^{0,0} = 1/2 \delta_{0, i \cdot j \bmod 2}$ with marginals $P_i^{0,\bullet} = P_j^{\bullet,0} = 1/2 \forall i, j$, yields the expression for the NSPR operator

$$O_{PR} = \frac{1}{4} [(\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) + (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) + (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) - (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) + I \otimes I], \quad (29)$$

where $\vec{m}_e = \sum_{i=0,1,2,\dots} \vec{m}_{2i}$, $\vec{m}_o = \sum_{i=0,1,2,\dots} \vec{m}_{2i+1}$, $\vec{n}_e = \sum_{j=0,1,2,\dots} \vec{n}_{2j}$, $\vec{n}_o = \sum_{j=0,1,2,\dots} \vec{n}_{2j+1}$.

In (29) the subscripts $\{e,o\}$ denote {even,odd} for the summation over even and odd dual measurement vectors. Note that in (29) the “single- σ ” terms $\sigma_i \otimes I$ and $I \otimes \sigma_j$ (representing measurements by Alice or Bob alone, respectively) have dropped out since the marginal distributions $P(a|x)=P(b|y)=1/2$ are independent of a, b, x, y . This leaves only the solely two-party correlation terms $\sigma_i \otimes \sigma_j$ and the maximally mixed term $(I \otimes I)/4$. For the bipartite case $n=2$ often considered in the literature for two qubits, each with two measurement directions $x \in \{\vec{m}_0, \vec{m}_1\}$ for Alice and $y = \{\vec{n}_0, \vec{n}_1\}$ for Bob (i.e. $a, b, x, y = \{0, 1\}$) we obtain the simplified form

$$O'_{PR} = \frac{1}{4} [(\vec{m}_0 \cdot \vec{\sigma}) \otimes (\vec{n}_0 \cdot \vec{\sigma}) + (\vec{m}_0 \cdot \vec{\sigma}) \otimes (\vec{n}_1 \cdot \vec{\sigma}) + (\vec{m}_1 \cdot \vec{\sigma}) \otimes (\vec{n}_0 \cdot \vec{\sigma}) - (\vec{m}_1 \cdot \vec{\sigma}) \otimes (\vec{n}_1 \cdot \vec{\sigma}) + I \otimes I]. \quad (30)$$

Using the procedure for calculating probabilities discussed after equation (30), the following probabilities can be computed from

$$\begin{array}{ccccc} \vec{n}_0 & \vec{n}_1 & \vec{n}_0 & \vec{n}_1 & \vec{n}_0 & \vec{n}_1 & \vec{n}_0 & \vec{n}_1 & \vec{n}_0 & \vec{n}_1 \\ \vec{m}_0 \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 0 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 0 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 0 & 0 \\ 0 & 1/2 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 0 & 0 \\ 0 & 1/2 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ \vec{m}_1 \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 0 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 0 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 0 & 0 \\ 0 & 1/2 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 0 & 0 \\ 0 & 1/2 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{array} \quad (31)$$

$P(a=0, b=0 | x=\vec{m}_i, y=\vec{n}_j), P(a=1, b=1 | \vec{m}_i, \vec{n}_j), P(a=0, b=1 | \vec{m}_i, \vec{n}_j), P(a=1, b=0 | \vec{m}_i, \vec{n}_j), E(\vec{m}_i, \vec{n}_j)$

$a \oplus b = 0, \quad a \oplus b = 1,$

$\Rightarrow P = 1/2 \text{ for } (x, y) \in \{(0,0), (0,1), (1,0)\}, \quad \Rightarrow P = 1/2 \text{ for } (x, y) \in \{(1,1)\}.$

Here, the correlations in (31) are computed as (see (5))

$$E(\vec{m}_i, \vec{n}_j)_{i,j \in \{0,1\}} = P(a=0, b=0 | x=\vec{m}_i, y=\vec{n}_j) + P(a=1, b=1 | \vec{m}_i, \vec{n}_j) - P(a=0, b=1 | \vec{m}_i, \vec{n}_j) - P(a=1, b=0 | \vec{m}_i, \vec{n}_j), \quad (32)$$

with corresponding S parameter (see (5))

$$S = E(\vec{m}_0, \vec{n}_0) + E(\vec{m}_0, \vec{n}_1) + E(\vec{m}_1, \vec{n}_0) - E(\vec{m}_1, \vec{n}_1) = 4 = S_{AM}, \quad (33)$$

achieving the algebraic maximum value $S_{AM} = 4$.

For the case of two qubits with $m=3$ measurement vectors $x \in \{\vec{m}_0, \vec{m}_1, \vec{m}_2\}$ for Alice and $y = \{\vec{n}_0, \vec{n}_1, \vec{n}_2\}$ for Bob (i.e. $a, b = \{0,1\}$, with $x, y = \{0,1,2\}$) we obtain from (22) the probabilities and correlations

$$\begin{array}{ccccc} \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_0 & \vec{n}_1 & \vec{n}_2 \\ \vec{m}_0 & \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix} & \vec{m}_0 & \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix} & \vec{m}_0 & \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & \vec{m}_0 & \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & \vec{m}_0 & \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \\ \vec{m}_1 & \begin{bmatrix} 1/2 & 0 & 1/2 \end{bmatrix} & \vec{m}_1 & \begin{bmatrix} 1/2 & 0 & 1/2 \end{bmatrix} & \vec{m}_1 & \begin{bmatrix} 0 & 1/2 & 0 \end{bmatrix} & \vec{m}_1 & \begin{bmatrix} 0 & 1/2 & 0 \end{bmatrix} & \vec{m}_1 & \begin{bmatrix} 1 & -1 & 1 \end{bmatrix} \\ \vec{m}_2 & \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix} & \vec{m}_2 & \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix} & \vec{m}_2 & \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & \vec{m}_2 & \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & \vec{m}_2 & \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \end{array} \quad (34)$$

$$P(a=0, b=0 | x=\vec{m}_i, y=\vec{n}_j), \quad P(a=1, b=1 | \vec{m}_i, \vec{n}_j), \quad P(a=0, b=0 | \vec{m}_i, \vec{n}_j), \quad P(a=1, b=0 | \vec{m}_i, \vec{n}_j), \quad E(\vec{m}_i, \vec{n}_j)$$

$$a \oplus b = 0,$$

$$a \oplus b = 1,$$

$$\Rightarrow P=1/2 \text{ for } (x, y) \in \{(e, e), (e, o), (o, e)\},$$

$$\Rightarrow P=1/2 \text{ for } (x, y) \in \{(o, o)\}.$$

In (27) $e = \{0,2\}$ denotes even indices of the measurement directions while $o = \{1\}$ denotes odd indices. We achieve the algebraic maximum for the S parameter, generalizing (33) defined as

$$S = E(\vec{m}_e, \vec{n}_e) + E(\vec{m}_e, \vec{n}_o) + E(\vec{m}_o, \vec{n}_e) - E(\vec{m}_o, \vec{n}_o) = 4 = S_{AM}. \quad (35)$$

Note that the dimension of the measurement vectors \vec{m}_i is set by the dimension $D = d^2 - 1$ of the Hilbert space of the observer, which simply states that any $(D+1) \times (D+1)$ matrix can be written in term of the $(D+1) \times (D+1)$ identity matrix and the D generators of $su(d)$. For qubits, $D=3$ and the three generators of $su(2)$ are the usual Pauli matrices $\vec{\sigma}$. For a given set of m measurement 3-vectors $\{\vec{m}_i\}$ (vectors in the Bloch sphere, $|\vec{m}_i| \leq 1$) one needs to solve for the correspond dual measurement vectors $\{\vec{m}_j\}$ satisfying $\vec{m}_i \cdot \vec{m}_j = \delta_{i,j}$. We write these equations as the matrix equation $\mathbf{M}_{m \times 3} \tilde{\mathbf{M}}_{3 \times m} = \mathbf{I}_{m \times m}$ where the i th row ($i = \{0,1,\dots,m-1\}$) of (the known coefficient matrix) $\mathbf{M}_{m \times 3}$ is \vec{m}_i , and the j th column of (unknowns) $\tilde{\mathbf{M}}_{3 \times m}$ is \vec{m}_j . By linear algebra, there exists a right inverse of $\mathbf{M}_{m \times 3}$ via $\tilde{\mathbf{M}}_{Right Inv} = \mathbf{M}^T (\mathbf{M} \mathbf{M}^T)^{-1}$ (if $(\mathbf{M} \mathbf{M}^T)^{-1}$ exists) if the columns of $\mathbf{M}_{m \times 3}$ span R^m , which can only occur for $m \leq D=3$. The systems of equations is under-determined and there exists at least one solution (typically and infinite number due to undetermined free parameters). This is the situation for probabilities and correlations shown in (31) and (34) for the case $m=2$ and $m=3$ measurement vectors, respectively. For the $m > D=3$, there exists at most one, unique solution (if any). This is the least squares (LS) solution using the pseudo-inverse $\mathbf{M}_{m \times 3}$ given by $\tilde{\mathbf{M}}_{LS} = (\mathbf{M}^T \mathbf{M})^{-1} \mathbf{M}^T$ (if $(\mathbf{M}^T \mathbf{M})^{-1}$ exists). In general, the LS solution has non-zero residual errors given by $\mathbf{Err} = \mathbf{M}_{m \times 3} \tilde{\mathbf{M}}_{LS(3 \times m)} - \mathbf{I}_{m \times m}$, corresponding to joint probabilities that may be negative for some measurements but still satisfy the (total probability) normalization condition $\sum_{a,b} P(a, b | x, y) = 1, \forall x, y$. Nonetheless, it is instructive to perform numerical searches in the case of $m > 3$ of random measurement vectors to seek solutions which yield all joint probabilities in the

range $0 \leq P(a,b|x,y) \leq 1$, for all pairs of measurement vectors \vec{m}_i, \vec{n}_j for Alice and Bob that still yield supra-correlations, i.e. $0 < S-S_Q \leq 4-2\sqrt{2} = 1.172$.

For the case $m=4$, a particular solution is shown in (36) that yields $S-S_Q = 0.102$ (for brevity, we only show $P(a=0, b=0 | x=\vec{m}_i, y=\vec{n}_j)$ and the correlations $E(\vec{m}_i, \vec{n}_j)$). In general, the even/odd structure of the correlations $E(\vec{m}_i, \vec{n}_j)$

$$\begin{array}{cccc}
 & \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_3 \\
 \vec{m}_0 & 0.237 & 0.395 & 0.072 & 0.406 \\
 \vec{m}_1 & 0.162 & 0.018 & 0.381 & 0.004 \\
 \vec{m}_2 & 0.469 & 0.449 & 0.341 & 0.457 \\
 \vec{m}_3 & 0.249 & 0.038 & 0.481 & 0.024
 \end{array} \Bigg], \quad
 \begin{array}{cccc}
 & \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_3 \\
 \vec{m}_0 & -0.052 & 0.581 & -0.710 & 0.623 \\
 \vec{m}_1 & -0.350 & -0.927 & 0.522 & -0.982 \\
 \vec{m}_2 & 0.875 & 0.796 & 0.365 & 0.829 \\
 \vec{m}_3 & -0.004 & -0.847 & 0.923 & -0.905
 \end{array} \quad (36)$$

$$P(a=0, b=0 | x=\vec{m}_i, y=\vec{n}_j), \quad E(\vec{m}_i, \vec{n}_j)$$

exhibited in the cases $m \leq 3$ ((31) and (34)) is destroyed, yet they still produce supra-correlations $S-S_Q \geq 0$. For each value of m in Figure 35 (left) we searched 10^5 random trials of the measurement vectors $\{\vec{m}_i, \vec{n}_j\}_{i,j \in \{0,1,\dots,m-1\}}$ and plot the value of $S-S_Q$ for the first solution encountered in which (i) we find proper joint probability distributions $0 \leq P(a,b | x=\vec{m}_i, y=\vec{n}_j) \leq 1$ for all measurement vectors, and (ii) which produce supra-correlations, $S-S_Q \geq 0$. In Figure 35 (middle), we plot the minimum

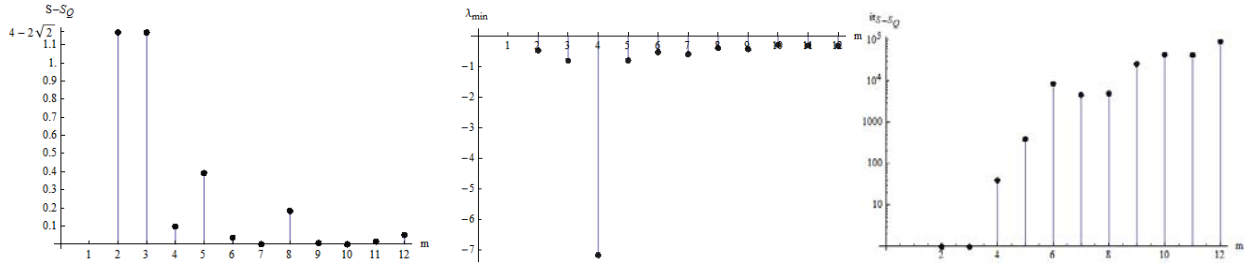


Figure 35. Numerical simulations for $m=\{2,3,4,\dots,12\}$ measurement vectors.

eigenvalue λ_{\min} of the matrix O in (29). The negative value of λ_{\min} indicates that O is not realized by a proper quantum state (i.e. a positive, Hermitian operator, $\rho \geq 0$). The rightmost plot in Figure 35 is the iteration number at which the first set of measurement vectors was found which produced supra-correlations. For the values of $13 \leq m \leq 20$ numerically explored, no supra-correlations solutions were found within 10^5 trials (the plot indicates that it becomes exponentially hard to find such a solution).

No Signaling (NS) Correlations: 3-Qubits

The bipartite results of the previous section for $n=2$ -qubits are straightforwardly extended to the tripartite case of $n=3$ -qubits with similar implications. Here the generalization of the bipartite CHSH nonlocality parameter S is given by the Svetlichny [Svetlichny87] inequality (SI) relating correlations $E(a,b,c|x,y,c)$ between three spacelike separated parties A, B, C

$$S \equiv E(a,b,c|0,0,0) + E(a,b,c|0,1,0) + E(a,b,c|1,0,0) - E(a,b,c|1,1,0) \\ + E(a,b,c|0,0,1) - E(a,b,c|0,1,1) - E(a,b,c|1,0,1) - E(a,b,c|1,1,1). \quad (37)$$

The SI has the bounds (i) $|S| \leq S_C = 4$ for classical correlations, (ii) $|S| \leq S_Q = 4\sqrt{2}$ for quantum correlations, with (iii) the algebraic upper bound given by $|S| \leq S_{AM} = 8$, achieved when the correlations in (37) take the values $E=1$ if they are preceded by a plus sign, and $E=-1$ if they are preceded by a minus sign. The generalization of the PR correlations of (37) is given by [Xiang11]

$$\text{TPR Box: } P(a,b,c|x,y,z) = \begin{cases} 1/4 & \text{if } a \oplus b \oplus c = x \cdot y \oplus y \cdot z \oplus x \cdot z \\ 0 & \text{otherwise} \end{cases}, \quad (38)$$

often referred to as a tripartite PR (TPR) box. The marginal distributions of (31) are again isotropic and satisfy the NS constraint, i.e. $P(a,b|x,y,z) = P(a,b|x,y) = 1/4$ for all a,b,x,y,z and $P(a,x,y) = P(a|x) = 1/2$ for all a,x,y , and similarly for all other marginal probability distributions.

For the case of $n=3$ qubits ($r=2$ output measurement values) $a,b,c = \{0,1\}$, with m possible measurement vectors for each observer, $x,y,z = \{0,1,\dots,m-1\}$ we again find that only the highest (three party) correlations term and the maximally mixed term are non-zero in the expression for O_{TPR}

$$O_{\text{TPR}} = \frac{1}{8} \left[\{(\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) + (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) + (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) - (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma})\} \otimes (\vec{r}_e \cdot \vec{\sigma}) \right. \\ \left. - \{(\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) + (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) + (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) - (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma})\} \otimes (\vec{r}_o \cdot \vec{\sigma}) + I \otimes I \otimes I \right], \quad (39)$$

where $\vec{q}_e = \sum_{i=0,1,2,\dots} \vec{q}_{2i}$, $\vec{q}_o = \sum_{i=0,1,2,\dots} \vec{q}_{2i+1}$, $\vec{q} = \{\vec{m}, \vec{n}, \vec{r}\}$.

The regular, even/odd (mod 2) structure of O_{TPR} in (39) reflects the non-zero structure of the TRP probabilities in (31), and can be seen as an additional single qubit generalization of O_{PR} in (29). That is, the 2-qubit term in the first curly brackets in (39) $\{(\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) + (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) + (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) - (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma})\}$ tensor-producted with the remaining “even” qubit term $(\vec{r}_e \cdot \vec{\sigma})$, is precisely two-party correlation term that appears in O_{PR} in (22). Similarly, the term in the second curly bracket in (39) $\{(\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) + (\vec{m}_o \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma}) + (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_o \cdot \vec{\sigma}) - (\vec{m}_e \cdot \vec{\sigma}) \otimes (\vec{n}_e \cdot \vec{\sigma})\}$ tensor-producted with the remaining “odd” qubit term $(\vec{r}_o \cdot \vec{\sigma})$ (with the accompanying minus sign) is just the bit flip ($e \leftrightarrow o$) of the previous two-party correlation term. Again, we can achieve the algebraic maximum $S_{AM}=8$ when each party has (for

the case of qubits) at most $m=3$ measurement vectors (for exactly the same linear algebraic reason for the $n=2$ bipartite case). Further, as in the bipartite case, we can find particular NS supra-correlation solutions $0 < S - S_Q \leq 4 - 2\sqrt{2}$ for $m > 3$, but which become increasingly hard to find the larger the value of m .

4.8 Efficient Cluster State Generation

To date most of experimental research on cluster state generation involves spontaneous parametric down-conversion (SPDC) for producing entangled photon pairs (consequently existing schemes are limited to completely stochastic non-heralded generation of cluster states). Cluster state generation is achieved by applying a standard optical CZ gate, with the success rate of $1/9$. The gate requires two additional vacuum ports i.e. the general scheme in Fig 2 will include two auxiliary vacuum ports. It has been demonstrated by finding direct analytic solution of a set of algebraic equation for transition amplitudes of basis states of two-qubit Hilbert space that the maximal success probability of optical CZ gate is equal to $1/9$.

C₄, C₆ and C₈ linear cluster state generation from Bell states

Since the complexity of the problem grows exponentially with the number of qubits involved in the transformation [Kok07], the problem of optimal generation of cluster states cannot be solved analytically even for the problem of generation of C₄ state. Therefore we resort to numerical methods developed in. From the point of view of quantum control theory the problem of cluster state generation is the problem of state control rather than control of a quantum transformation acting in a Hilbert space. Therefore full CZ gates may not be the optimal way to generate a cluster state from a specific initial state. This phenomenon has been already confirmed for transformations involving concatenation of several CNOT gates and this idea is being exploited in the present work.

In our studies the input state for generating C₄, C₆ and C₈ linear clusters was taken to be a tensor product of two, three and four Bell states correspondingly $|\Psi_4^{(in)}\rangle = |\Phi^+\rangle_{1,2} |\Phi^+\rangle_{3,4}$, $|\Psi_6^{(in)}\rangle = |\Phi^+\rangle_{1,2} |\Phi^+\rangle_{3,4} |\Phi^+\rangle_{5,6}$, $|\Psi_8^{(in)}\rangle = |\Phi^+\rangle_{1,2} |\Phi^+\rangle_{3,4} |\Phi^+\rangle_{5,6} |\Phi^+\rangle_{7,8}$, where $|\Phi^+\rangle_{n,m} \equiv (|H\rangle_n |H\rangle_m + |V\rangle_n |V\rangle_m) / \sqrt{2}$. We note that Bell State $|\Phi^+\rangle$ can be morphed into a canonical C₂ cluster state $|C_2\rangle_{n,m} = (|H\rangle_n |H\rangle_m + |H\rangle_n |V\rangle_m + |V\rangle_n |H\rangle_m - |V\rangle_n |V\rangle_m) / 2$ by a deterministic local unitary transformation acting on polarization modes $a_{H,m}^\dagger \rightarrow (\tilde{a}_{H,m}^\dagger + \tilde{a}_{V,m}^\dagger) / \sqrt{2}$, $a_{V,m}^\dagger \rightarrow (\tilde{a}_{H,m}^\dagger - \tilde{a}_{V,m}^\dagger) / \sqrt{2}$. The target states are taken to be a canonical cluster states generated by applying an abstract two-qubit entangling CZ gate between neighboring qubits prepared in a so-called "plus" states $|\psi^+\rangle = (|H\rangle + |V\rangle) / \sqrt{2}$.

Our numerical results show excellent convergence to a global maximum (see Figure 36a, b below). In principle, linear optical transformation may be extended to a broader class of non-

unitary matrices U . The subsequent implementation of such a matrix in the form of a linear optical device requires dilation of a non-unitary matrix to a unitary matrix by adding extra modes, called vacuum modes (i.e. modes carrying zero input photons as shown in see Fig. 13). Our search in the space of non-unitary matrices shows that solutions with success probability larger than 0.16 are automatically unitary.

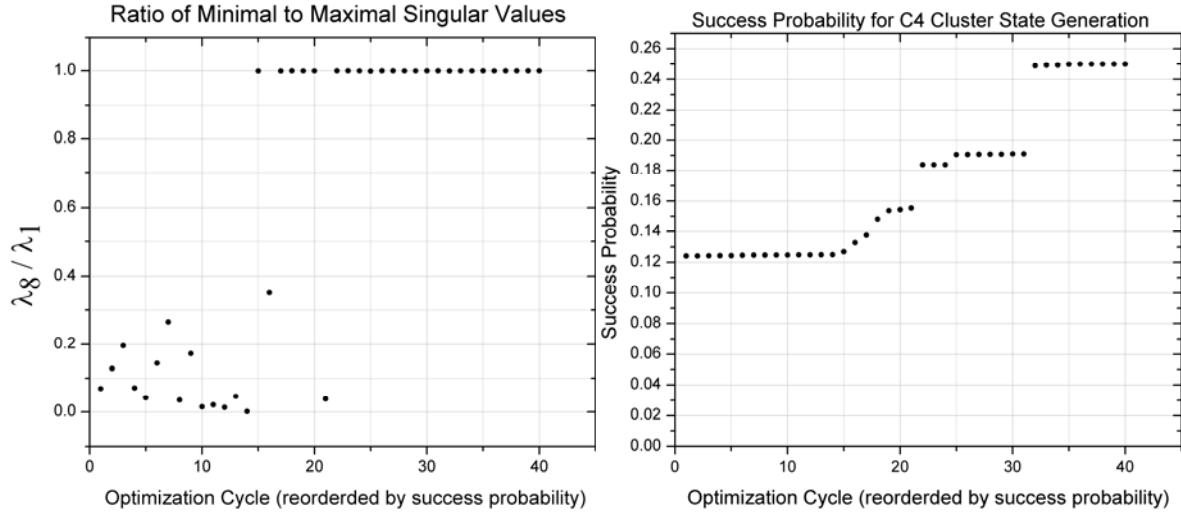


Figure 36 Numerical results for generation of C_4 cluster state from a pair of two Bell states. (left) ratio of smallest to largest singular value of transformation matrix, (right) success probability.

Figure 36 (left) shows the ratio of the smallest singular value of a transformation matrix to the largest singular value. If the ratio is equal to 1 then all singular values are equal to one and the matrix is unitary. These results are obtained for generation of C_4 cluster state from a pair of two Bell states. Figure 36 (right) shows the success probability for generation of linear C_4 cluster state from a pair of Bell states: a sample of 40 optimization cycles reordered by increasing success probability (overall we accumulated statistics for more than 2000 cycles confirming that $s=1/4$ is the global maximum). The result in Figure 36 (right) immediately demonstrates that the standard scheme of cluster state generation using a destructive CZ gate to fuse two photonic Bell states is not optimal. The success probability can be improved by a factor of 9/4 by modifying the linear optical part of the experimental setup.

Our next results for C_6 and C_8 are shown in Figure 37 (left) and Figure 37 (right).

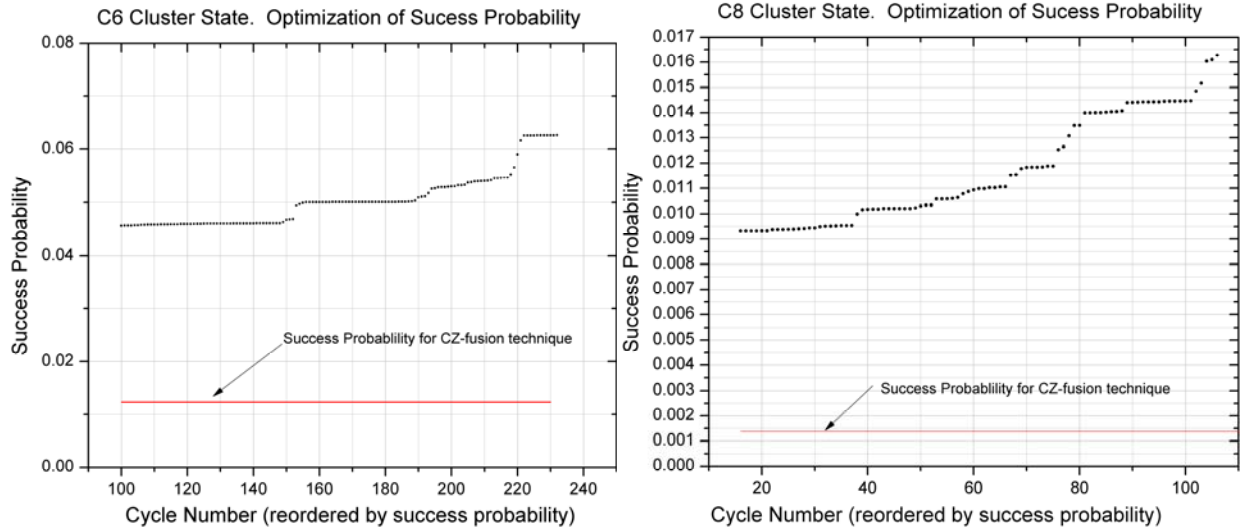


Figure 37. Success probability for C_6 (left) and C_8 (right) cluster state generation from three Bell states. The maximum probability is (left) $s=(1/4)^2$, (right) $s=(1/4)^3$.

Figure 37 (left) shows the results of the optimization of the C_6 cluster state generation from three Bell states. The y-axis shows the value of success probability. The maximal success probability $s=(1/4)^2$. Figure 37 (right) shows the results of the optimization of the C_8 cluster state generation from three Bell state pairs of photonic qubits. The y-axis shows the value of success probability. The maximal success probability is numerically close to $s = (1/4)^3$.

We observe that the maximal success probability for the C_6 cluster state is numerically very close to $0.0625 = 1/4^2$. Since the numerical complexity of multiphoton optimization problem grows super-exponentially with the number of photons we were able to find only a few local maxima for the C_8 cluster state generation problem. However the general trend of numerical results for the set of C_4 , C_6 and C_8 states indicates that the maximal success probability for generation of a C_n linear cluster state (here n indicates the number of qubits in a cluster) from $n/2$ photonic Bell states depends on the number of additional fusion links $m = n/2 - 1$ as $1/4^m$. For the C_4 cluster state this number is 1, for the C_6 cluster state $m=2$ and for the C_8 cluster state $m=3$. Due to the increasing numerical complexity of global optimization and we were not able to verify this result for cluster states larger than C_8 . However, our results demonstrate that the computational advantage of the optimal scheme grows exponentially fast with the size of the cluster state. For the C_4 cluster state generation we obtain a factor of $9/4$ improvement compared with the traditional scheme; for the C_6 cluster state this factor is $(9/4)^3 \approx 5$; and for the C_8 cluster state the improvement factor is $(9/4)^3 \approx 11$. Based upon these results we expect that for higher-dimensional states the advantage of the optimal scheme will continue to grow as a power of $9/4$.

C4, C6 and C8 cluster state generation from product states

In this section we describe the numerical results of fidelity-constrained optimization of success probability by presenting the data on optimization of success probability for cluster state generation from product states. In contrast with the previous section the initial state does not contain any “pre-loaded” entanglement as in Bell states and one expects that success probability of generating a cluster state, where entanglement permeates the whole cluster, will be reduced. Surprisingly this common-sense reasoning turns out to be incorrect. Our results can be concisely formulated as follows: the success probability of generating a C_n cluster state from n -photon product states is only a factor of 2 smaller than maximal success probability of generating a C_n cluster state from $n/2$ -tuple of Bell states.

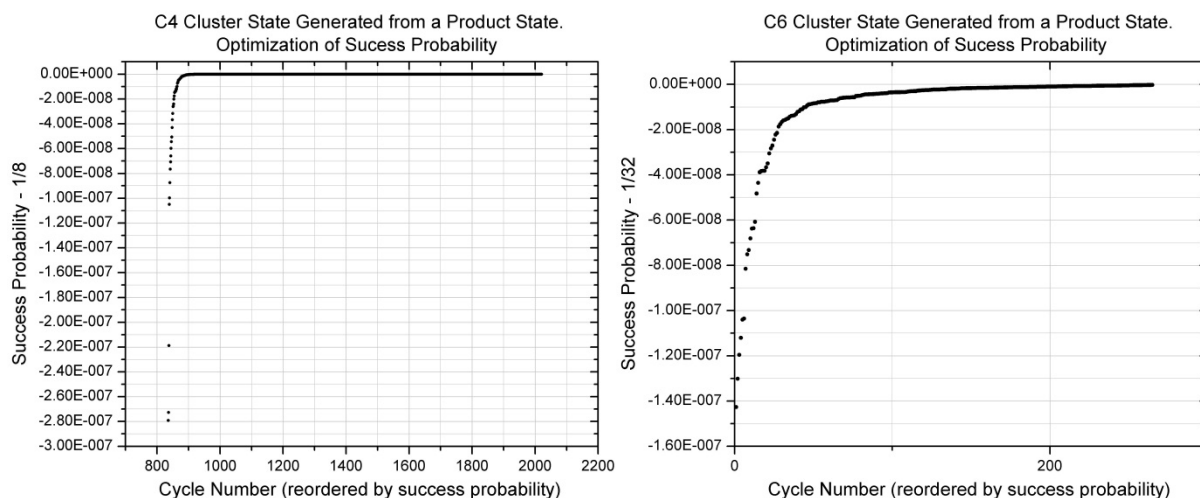


Figure 38. Success probability for C_4 (left) and C_6 (right) cluster state generation from product states. The maximum probability is (left) $s=(1/2)^3$, (right) $s=(1/2)^5$.

Figure38 (left) shows the results of the optimization of the $|C_4\rangle$ cluster state generation from a product state. The y-axis shows the value of success probability minus its maximal value of $1/8$. Figure 38 (right) shows the results of the optimization of the $|C_6\rangle$ cluster state generation from a product state. The y-axis shows the value of success probability minus its maximal value of $1/32$.

Unfortunately the structure of optimal solutions encoded in the linear optical matrix U is too complicated to allow simple analysis of the underlying mechanisms of this phenomenon for general solutions. However power-law dependence of the success rate of optimal fusion transformations strongly suggests that in the process of fusing a Bell state to a C_n cluster the entanglement of the Bell state does not help to increase the success probability of the operation. In other words, we expect that sequential fusion of two unentangled single-photon states to C_n cluster state, resulting in C_m cluster state with $m=n+2$, can be implemented with the same efficiency as fusion of a Bell state to C_n cluster state.

Table 2. Results of success probability of cluster state generation (with combined results for C_3 and C_5)

	C_2	C_3	C_4	C_5	C_6	C_7	C_8
From Bell Pairs (optimal)	1	n/a	1/4	n/a	1/16	n/a	1/64
From n-qubit Product state (optimal)	1/2	1/4	1/8	1/16	1/32	1/64	1/128
Fusion by CZ gate from product state	1/9	1/81	1/729	1/6561	1/59049	1/531441	1/4782969
Fusion by CZ gate from Bell pairs	n/a	n/a	1/9	n/a	1/81	n/a	1/729

We performed numerical analysis of the problem of photonic cluster-state generation in application to quantum optics. Our method performs a search for the most efficient scheme of cluster state generation from either a combination of untangled photons or a set of pairs of entangled photons.

The optimization tasks we performed are of critical importance for photonic quantum computation since the only photon-photon entangling operations currently implementable with high repetition rate and fidelity are measurement-assisted stochastic quantum transformations. Our results demonstrate that standard methods of cluster state generation using standard probabilistic linear optical CZ (C-phase) gate is far from optimal. Performing numerical optimization we established that there exists a scheme of cluster state generation which boosts the success rate of generation by more than an order of magnitude even for a small eight-qubit cluster state. The advantage of this scheme in comparison with traditional schemes grows exponentially fast with the size of a cluster.

Finding the simplest possible realization of the scheme with the fewest number of optical elements requires further analytical and numerical analysis for which we some preliminary details below. Further details can be found in [Uskov13, Uskov14].

Towards an explanation of the numerical results

To explain the observed dependence of fusion success probability on the number (and structure) of qubit states we first introduce a generic fusion gate by relaxing the standard CZ gate. Formally the CZ gate is a linear operator acting in 2-qubit C^4 Hilbert space as specified by equation (5). It preserves the Hermitian scalar product and as such belongs to the $U(4)$ group. Let us first fix the

notation for qubits encoded in photon polarization states: as mentioned above we will assume that qubit logical states $|0\rangle$ and $|1\rangle$ are conventionally encoded in horizontal $|H\rangle$ and vertical $|V\rangle$ polarization states of a photon correspondingly. Linear combinations of these states are denoted as $|\psi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$.

Consider first a fusion of a C_n cluster with a single qubit:

$$|C_n\rangle |\psi^+\rangle_{n+1} \rightarrow |C_{n+1}\rangle \quad (40)$$

In the above equation we assume for simplicity that $(n+1)$ th qubit is prepared in the $|\psi^+\rangle$ state. The fusion transformation (40) does not have to be implemented via a unitary transformation: it can be any general SLOCC transformation. Now notice that when “fusing” a *single* qubit with n -qubit cluster one strictly speaking does not work with operators acting in two-qubit \mathbf{C}^4 space. Since the state of an extra $(n+1)$ th qubit is always fixed, all operators are in fact acting on the \mathbf{C}_{in}^2 subspace of \mathbf{C}^4 spanned by states $|V\rangle_n |\psi^+\rangle_{n+1}$ and $|H\rangle_n |\psi^+\rangle_{n+1}$, mapping this subspace onto the full \mathbf{C}^4 space. Such operators do not form a Lie group; instead they belong to the so-called Stiefel space $V_2(\mathbf{C}^4)$ [Porteous95]. If the action of an operator from $V_2(\mathbf{C}^4)$ on $\mathbf{C}_{in}^2 = \text{Span}\{|H\rangle_n |\psi^+\rangle_{n+1}, |V\rangle_n |\psi^+\rangle_{n+1}\}$ is identical to the action of a CZ gate on \mathbf{C}_{in}^2 then such an operator will fuse an additional qubit to any C_n cluster forming a larger C_{n+1} cluster state. Let us denote such an operator as CZ_V to distinguish it from the CZ gate itself. This operator must satisfy two equations determining its action in \mathbf{C}_{in}^2

$$\begin{aligned} CZ_V |H\rangle_n |\psi^+\rangle_{n+1} &= CZ |H\rangle_n |\psi^+\rangle_{n+1} \equiv \frac{1}{\sqrt{2}}(|H\rangle_n |H\rangle_{n+1} + |H\rangle_n |V\rangle_{n+1}), \\ CZ_V |V\rangle_n |\psi^+\rangle_{n+1} &= CZ |V\rangle_n |\psi^+\rangle_{n+1} \equiv \frac{1}{\sqrt{2}}(|V\rangle_n |H\rangle_{n+1} - |V\rangle_n |V\rangle_{n+1}). \end{aligned} \quad (41)$$

In the context of photonic entangling gates conditioned on coincidence multimode photon detection one should further relax the requirement on the fusion operation by adding a scaling factor α and introducing extra terms in equations (41)

$$\begin{aligned} CZ_V^{LO} |H\rangle_n |\psi^+\rangle_{n+1} &= \alpha \frac{1}{\sqrt{2}}(|H\rangle_n |H\rangle_{n+1} + |H\rangle_n |V\rangle_{n+1}) + |\Psi_H^H\rangle, \\ CZ_V^{LO} |V\rangle_n |\psi^+\rangle_{n+1} &= \alpha \frac{1}{\sqrt{2}}(|V\rangle_n |H\rangle_{n+1} - |V\rangle_n |V\rangle_{n+1}) + |\Psi_V^H\rangle. \end{aligned} \quad (42)$$

To distinguish an abstract CZ operator satisfying equations (41) from a linear optical transformation (42) we use the notation CZ_V^{LO} . Additional terms in equations (42), denoted as $|\Psi_{H,V}^H\rangle$, are states from a space complementary (orthogonal) to the space of the dual-rail

encoding. These functions are normalized as $\langle \Psi_H'' | \Psi_H'' \rangle = \langle \Psi_V'' | \Psi_V'' \rangle = \sqrt{1 - |\alpha|^2}$ and if all measurement operations on photonic cluster qubits are successful these states vanish. Probability of such a scenario according to the Born rule is equal to $|\alpha|^2$. While operators satisfying equations (41) cannot be implemented by linear optics and require non-linear photon-photon coupling (such as cross-Kerr non-linearity), those operators satisfying equations (42) may be implemented by linear optics and photo-counting measurement operations.

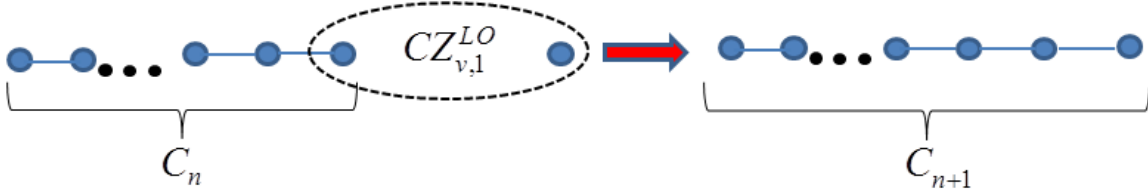


Figure 39. Fusing a single qubit to a C_n cluster.

The first theoretical scheme of a linear-optical CZ^{LO} gate in the coincidence basis was described by Ralph *et al.* [Ralph02] and implemented experimentally using specially engineered Polarization Beam Splitters (PBS) [Langford05, Kiesel05a, Kiesel05b, Okamoto05]. This gate satisfies a set of four equations

$$\begin{aligned} CZ^{LO} |H\rangle_1 |H\rangle_2 &= \frac{1}{3} |H\rangle_1 |H\rangle_2 + |\Psi_{HH}''\rangle, & CZ^{LO} |H\rangle_1 |V\rangle_2 &= \frac{1}{3} |H\rangle_1 |V\rangle_2 + |\Psi_{HV}''\rangle, \\ CZ^{LO} |V\rangle_1 |H\rangle_2 &= \frac{1}{3} |V\rangle_1 |H\rangle_2 + |\Psi_{VH}''\rangle, & CZ^{LO} |V\rangle_1 |V\rangle_2 &= -\frac{1}{3} |V\rangle_1 |V\rangle_2 + |\Psi_{VV}''\rangle. \end{aligned} \quad (43)$$

If a transformation satisfies the set of equations (43), then it also will be a solution for the set of equations (42). An important relevant observation: the class of solutions for the set of equations (42) is larger than the class of solutions for equations (43). Formally, all these classes can be viewed as affine varieties [VanMeter07].

The CZ^{LO} solution suggested in [Ralph02, Hoffmann02] provided success probability $|\alpha|^2 = 1/9$. It was demonstrated recently [Kieling10, Lemr11] by finding the direct algebraic solution for the matrix of linear optical transformations that this is the maximal possible success probability for a CZ^{LO} gate and it cannot be improved by modifying the optical scheme. This fact makes such a gate frustratingly inefficient when applied multiple times to produce high-dimensional clusters. Therefore in practice larger photonic cluster states are generated by fusing photonic Bell states produced by SPDC [Walther05, Yao12] (see also references in the review paper [Pan12]). For example, the production of a C_4 cluster out of four independent qubits will require three applications of a CZ^{LO} gate with resulting success probability of $(1/9)^3$ while generation of the same C_4 state out of two photonic Bell pairs requires only one application of the CZ^{LO} gate with the resulting success probability of $(1/9)$. This approach follows a common wisdom based on an

expectation that entanglement contained in the initial photonic Bell pairs will help to increase the rate of production of cluster states. One counterintuitive conclusion of our work is that this type of reasoning is actually wrong: if one is using the optimal scheme of cluster generation the rate of production of cluster states does not increase when more entanglement resources are invested in the preparation of the initial state. A set of purely separable photonic qubits provides the same success probability as Bell states. So, a natural belief that SPDC producing polarization entangled photons will help to generate cluster states in linear optical approach seems to be incorrect.

An additional resource which we are using here is exploiting the fact that the class of CZ_v^{LO} transformations is larger than canonical CZ^{LO} . While CZ^{LO} cannot be made more efficient than $|\alpha|^2 = 1/9$, we can make CZ_v^{LO} as efficient as $|\alpha|^2 = 1/2$. Yet, there is a price to pay: CZ_v^{LO} will work only for fusing a separate qubit to a cluster state (any cluster state) because it exploits the fact that a qubit to be fused to a cluster is prepared in a specific state, which for simplicity, we assume to be a “plus” state $|\psi^+\rangle_{n+1} \equiv \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$.

Adding qubit to the *end* of the linear cluster state

The following calculation demonstrates how the mapping given by the two equations in (41) is unique. Working through this calculation also illuminates the role of the entanglement of the linear cluster state forcing the uniqueness of the mapping.

Goal: we seek a state transformation that maps $|\psi_{in}\rangle = |C_n\rangle|+\rangle_{n+1} \rightarrow |C_{n+1}\rangle = |\psi_{out}\rangle$.

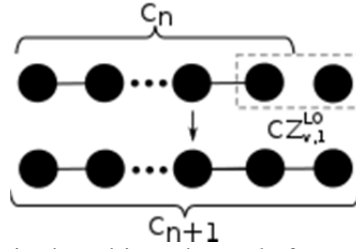


Figure 40: Fusion of a single qubit to the *end* of an n -qubit linear cluster state.

Let us note that we can write the n -qubit *linear* cluster state as $|C_n\rangle = 1/\sqrt{2^n} \sum_{i_1, \dots, i_n} (-1)^{i_1 i_2} \dots (-1)^{i_{n-1} i_n} |i_1, \dots, i_n\rangle$ where each index $i_k \in \{0, 1\} \leftrightarrow \{H, V\}$.

Let us expand the input state $|\psi_{in}\rangle = |C_n\rangle|+\rangle_{n+1}$ on qubits n and $n+1$ as

$$\begin{aligned} |\psi_{in}\rangle &= |C_n\rangle|+\rangle_{n+1} = 1/\sqrt{2^n} \sum_{i_1, \dots, i_n} (-1)^{i_1 i_2} \dots (-1)^{i_{n-1} i_n} |i_1, \dots, i_n\rangle|+\rangle_{n+1} \\ &= 1/\sqrt{2^n} \sum_{i_1, \dots, i_{n-1}} (-1)^{i_1 i_2} \dots (-1)^{i_{n-2} i_{n-1}} |i_1, \dots, i_{n-1}\rangle (|0_n\rangle|+\rangle_{n+1} + (-1)^{i_{n-1}} |1_n\rangle|+\rangle_{n+1}). \end{aligned} \quad (44)$$

Note: in the last line of (44) rightmost parentheses, the $n, n+1$ qubit term $(-1)^{i_{n-1}} |1_n\rangle |_{-_{n+1}}\rangle$ contains the phase information from the $CZ_{n-1,n}$ link between qubits $n-1$ and n . (Note: $(-1)^{i_{n-1}(i_n=0)} = 1$ and $(-1)^{i_{n-1}(i_n=1)} = (-1)^{i_{n-1}}$). It turns out this will force the uniqueness of the mapping given in (41).

Now let us similarly expand the output state $|\psi_{out}\rangle = |C_{n+1}\rangle$ on qubits $n, n+1$ (combining four terms into two):

$$\begin{aligned} |\psi_{out}\rangle &= |C_{n+1}\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{i_1, \dots, i_n} (-1)^{i_1 i_2} \dots (-1)^{i_{n-1} i_n} (-1)^{i_{n+1}} |i_1, \dots, i_n, i_{n+1}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{i_1, \dots, i_{n-1}} (-1)^{i_1 i_2} \dots (-1)^{i_{n-2} i_{n-1}} |i_1, \dots, i_{n-1}\rangle (|0_n\rangle |_{+_{n+1}}\rangle + (-1)^{i_{n-1}} |1_n\rangle |_{-_{n+1}}\rangle). \end{aligned} \quad (45)$$

Comparing the terms in the rightmost (...) in (44) and (45) we see that the mapping $CZ_{v,1}^{LO}$ needs to map

$$CZ_{v,1}^{LO} (|0_n\rangle |_{+_{n+1}}\rangle + (-1)^{i_{n-1}} |1_n\rangle |_{+_{n+1}}\rangle) = |0_n\rangle |_{+_{n+1}}\rangle + (-1)^{i_{n-1}} |1_n\rangle |_{-_{n+1}}\rangle. \quad (46)$$

The simplest, most direct mapping is given by (41) in the paper:

$$\begin{aligned} (i) \quad CZ_{v,1}^{LO} |0_n\rangle |_{+_{n+1}}\rangle &= |0_n\rangle |_{+_{n+1}}\rangle \\ (ii) \quad CZ_{v,1}^{LO} |1_n\rangle |_{+_{n+1}}\rangle &= |1_n\rangle |_{-_{n+1}}\rangle, \end{aligned} \quad (47)$$

in which the phase factor $(-1)^{i_{n-1}}$ appearing on both sides of (ii) in (47) cancels. Equation (47) then represents a 2-qubit transformation on qubits $n, n+1$.

Alternatively, from (46) we could (perversely) consider the (cross-term) mapping

$$\begin{aligned} (i') \quad CZ_{v,1}^{LO} |0_n\rangle |_{+_{n+1}}\rangle &= (-1)^{i_{n-1}} |1_n\rangle |_{-_{n+1}}\rangle = |1_n\rangle |_{-_{n+1}}\rangle; \quad = -|1_n\rangle |_{-_{n+1}}\rangle \\ &\quad (i_{n-1} = 0); \quad (i_{n-1} = 1); \\ (ii') \quad CZ_{v,1}^{LO} |1_n\rangle |_{+_{n+1}}\rangle &= (-1)^{i_{n-1}} |0_n\rangle |_{+_{n+1}}\rangle = |0_n\rangle |_{+_{n+1}}\rangle; \quad = -|0_n\rangle |_{+_{n+1}}\rangle. \end{aligned} \quad (48)$$

This form of the transformation depends on the value of i_{n-1} , so at minimum it would have to be implemented as a 3-qubit gate, with qubit $n-1$ acting as further control qubit. It could not be realized as a 2-qubit transformation.

The salient point of the above calculations is that the phases resulting from the CZ linkages of the qubit in question (here n) to neighboring qubits (here $n-1$) play a crucial role in determining the uniqueness of the mapping on the Stiefel space. The generalization of these results to 2D cluster states is currently under investigation.

Adding a qubit to the *middle* of the linear cluster state

Here we want to develop the Stiefel space equations on 3-qubits for adding a single qubit k to the middle of an n -qubit cluster state where $1 < k < n$, i.e. $|\psi_{in}\rangle = |C_n\rangle |_{+}\rangle_k \rightarrow |C_{n+1}\rangle = |\psi_{out}\rangle$. We know this can be accomplished with three CZ gates (with probability $(1/9)^3$) as

$|\psi_{out}\rangle = |C_{n+1}\rangle = CZ_{j_k, i_{k+1}} CZ_{i_{k-1}, j_k} CZ_{i_{k-1}, i_{k+1}} |C_n\rangle |+\rangle_k$ where $CZ_{i_{k-1}, i_{k+1}}$ breaks the existing link between qubits $k-1$ and $k+1$, and $CZ_{j_k, i_{k+1}} CZ_{i_{k-1}, j_k}$ establishes the new links between qubits $k-1$ and k , and k and $k+1$. We would like to do better than the standard $(1/9)^3$ success probability.

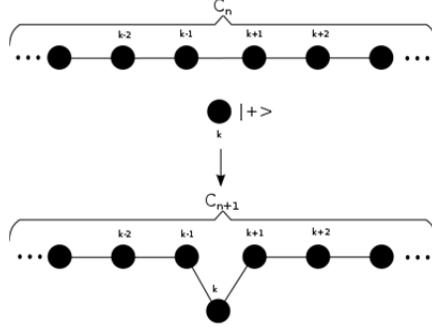


Figure 41: Fusion of a single qubit to the *middle* of an n -qubit linear cluster state.

Let label the n -qubit cluster state as $|C_n\rangle = 1/\sqrt{2^n} \sum_{i_1, \dots, i_{k-1}, i_{k+1}, i_{n+1}} (-1)^{i_1 i_2} \dots (-1)^{i_{k-1} i_{k+1}} (-1)^{i_{n+1} i_n} |i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_{n+1}\rangle$ with indice i_k absent.

After expanding on qubits $k-1, k, k+1$, we have

$$\begin{aligned} |\psi_{in}\rangle &= |C_n\rangle |+\rangle_k = 1/\sqrt{2^n} \sum_{i_1, \dots, i_{k-1}, i_{k+1}, i_{n+1}} (-1)^{i_1 i_2} \dots (-1)^{i_{k-1} i_{k+1}} (-1)^{i_{n+1} i_n} |i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_{n+1}\rangle \\ &= 1/\sqrt{2^n} \sum_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}} |\varphi_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}}\rangle \sum_{i_{k-1}, i_k, i_{k+1}} (-1)^{i_{k-2} i_{k-1}} (-1)^{i_{k-1} i_k} (-1)^{i_{k+1} i_{k+2}} |i_{k-1}\rangle |+\rangle_k |i_{k+1}\rangle \\ &= 1/\sqrt{2^{n-2}} \sum_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}} |\varphi_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}}\rangle \frac{1}{\sqrt{2}} \left(|0_{k-1}\rangle |+\rangle_k \frac{1}{\sqrt{2}} [|0_{k+1}\rangle + (-1)^{i_{k+2}} |1_{k+1}\rangle] + (-1)^{i_{k-2}} |1_{k-1}\rangle |+\rangle_k \frac{1}{\sqrt{2}} [|0_{k+1}\rangle - (-1)^{i_{k+2}} |1_{k+1}\rangle] \right) \end{aligned} \quad (49)$$

where, for convenience we have define

$$|\varphi_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}}\rangle \equiv (-1)^{i_1 i_2} \dots (-1)^{i_{k-3} i_{k-2}} (-1)^{i_{k+2} i_{k+3}} \dots (-1)^{i_{n+1} i_n} |i_1, \dots, i_{k-2}, i_{k+2}, \dots, i_{n+1}\rangle.$$

Similarly, we now expand the output state $|\psi_{out}\rangle = |C_{n+1}\rangle$ on qubits $k-1, k, k+1$, as

$$\begin{aligned} |\psi_{out}\rangle &= |C_{n+1}\rangle = 1/\sqrt{2^{n+1}} \sum_{i_1, \dots, i_n} (-1)^{i_1 i_2} \dots (-1)^{i_n i_{n+1}} |i_1, \dots, i_{n+1}\rangle \\ &= 1/\sqrt{2^n} \sum_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}} |\varphi_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}}\rangle \sum_{i_{k-1}, i_k, i_{k+1}} (-1)^{i_{k-2} i_{k-1}} (-1)^{i_{k-1} i_k} (-1)^{i_{k+1} i_{k+2}} |i_{k-1}\rangle |i_k\rangle |i_{k+1}\rangle \\ &= 1/\sqrt{2^{n-2}} \sum_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}} |\varphi_{i_1, \dots, i_{k-2}, i_{k+2}, i_{n+1}}\rangle \frac{1}{\sqrt{2}} \left(|0_{k-1}\rangle \frac{1}{\sqrt{2}} [|+\rangle_k |0_{k+1}\rangle + (-1)^{i_{k+2}} |-\rangle_k |1_{k+1}\rangle] + (-1)^{i_{k-2}} |1_{k-1}\rangle \frac{1}{\sqrt{2}} [|-\rangle_k |0_{k+1}\rangle + (-1)^{i_{k+2}} |+\rangle_k |1_{k+1}\rangle] \right). \end{aligned} \quad (50)$$

Comparing the terms in the right most parentheses in (49) and (50) we are led to the mapping

$$\begin{array}{ccc}
& \text{IN} & \text{OUT} \\
(i) & |0_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle & \rightarrow |0_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle, \\
(ii) & (-1)^{i_{k+2}}|0_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle & \rightarrow (-1)^{i_{k+2}}|0_{k-1}\rangle|-_k\rangle|1_{k+1}\rangle, \\
(iii) & (-1)^{i_{k-2}}|1_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle & \rightarrow (-1)^{i_{k-2}}|1_{k-1}\rangle|-_k\rangle|0_{k+1}\rangle, \\
(iv) & -(-1)^{i_{k-2}}(-1)^{i_{k+2}}|1_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle & \rightarrow (-1)^{i_{k-2}}(-1)^{i_{k+2}}|1_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle.
\end{array} \tag{51}$$

The most important points about (51) are that (a) the phases drop out from both sides of the mapping yielding

$$\begin{array}{ccc}
& \text{IN} & \text{OUT} \\
(i) & |0_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle & \rightarrow |0_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle, \\
(ii) & |0_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle & \rightarrow |0_{k-1}\rangle|-_k\rangle|1_{k+1}\rangle, \\
(iii) & |1_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle & \rightarrow |1_{k-1}\rangle|-_k\rangle|0_{k+1}\rangle, \\
(iv) & -|1_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle & \rightarrow |1_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle,
\end{array} \tag{52}$$

Independent of the CZ phase linkages of qubit $k-1$ to $k-2$ and qubit $k+1$ to $k+2$, and (b) we have 4 equations in (52) as opposed to $2^3 = 8$ equations for a full 3-qubit unitary, transforming the eight 3-qubit basis states consisting of the union of

$$\begin{aligned}
V_4^{(+)}(\mathbf{C}^8) &= \{|0_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle, |0_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle, |1_{k-1}\rangle|+_k\rangle|0_{k+1}\rangle, |1_{k-1}\rangle|+_k\rangle|1_{k+1}\rangle\} \text{ and} \\
V_4^{(-)}(\mathbf{C}^8) &= \{|0_{k-1}\rangle|-_k\rangle|0_{k+1}\rangle, |0_{k-1}\rangle|-_k\rangle|1_{k+1}\rangle, |1_{k-1}\rangle|-_k\rangle|0_{k+1}\rangle, |1_{k-1}\rangle|-_k\rangle|1_{k+1}\rangle\}.
\end{aligned}$$

Though it has not been proven yet, we suspect that we would get some improvement over the standard $(1/9)^3$ success probability utilizing three CZ gates. Additional research has been submitted for publication to Physical Review Letters [Uskov13b].

5.0 CONCLUSIONS

Multipli-entangled photons from a spontaneous parametric down-conversion source

This report describes research on the Schioedtei source, a unique type II SPDC source design for which additional in-depth information can be obtained through our previously published papers [Fanto11, Peters12]. Schioedtei generates up to six pairs of entangled photons per pass through the type II crystal assembly. This configuration surpasses the typical single entangled pair generated per pass found in standard type II SPDC sources. Concurrently Schioedtei generates a variety of states atypical of being produced from a single photon source. Useable photon generation rates (two and four photon) have been observed, thus showing its feasibility as a direct generation source of entangled photons for quantum optics/entanglement experiments. The six pairs of photons produced are directly applicable to the generation of linear, box, butterfly and a multitude of other cluster states. The utility of the Schioedtei source is (i) its reduced experimental footprint compared to standard multi-crystal/multi-pass experiments; (ii) it generates a variety of entangled/separable states; (iii) generated states are amenable towards cluster state generation. Furthermore, the generated photons from Schioedtei are the input states for our bulk optical gates and QPICs.

A path toward experimental generation of a linear cluster state

We successfully measured two entangled pairs of photons using the new mirror based collection system. We were able to improve the environmental controls for the crystal, and the polarization stabilization of transported photons, both critical components of the experimental test bed. Continuing to ensure the polarization of the photons is maintained when transporting photons is critical to future experiments. These accomplishments will allow for the creation of a linear four qubit cluster state and then a box cluster state. Those two states are the fundamental necessary building blocks to perform universal one-way quantum computing.

A multi-layer three dimensional superconducting nanowire photon detector

The multilayer superconducting number-resolving photon detector represents a significant improvement on current single layer meander devices. The device will have significantly higher number resolution, while maintaining a useful detection area. It has several parameters which can control the reset time to avoid latching while still minimizing the rest time. An array of pixels of arbitrary number, size and shape is possible. The active area of the detector can be tuned by changing the number or the shapes of the pixels. The fill factor of the detector should be at least equal to that of current nanowire meanders and given the potential reduction of the current crowding effect significantly higher. As a final note we will point out that the multi-layer superconducting number-resolving photon detector can also give a rough spatial distribution of the incident photons. These advantages are compelling evidence for the construction and testing of multi-layer superconducting number-resolving photon detectors.

Probabilistic cluster state generator patent

Single and entangled photons utilized for cluster state generation are difficult to generate in large quantities. This is due to the lack of availability of on demand single and entangled photon sources. Therefore taking advantage of the photons that are produced is critical. Any path towards the generation of an on-demand or periodic source of single or entangled photons is of tremendous benefit. The sequential entangler allows for the generation of cluster states in an efficient manner from a spontaneous photon source. Employing entangling gates which use the photons generated via spontaneous parametric downconversion as an input, the circuit generates the cluster state in a periodic manner. The further advancement beyond the one-dimensional cluster state is to generate 2-dimensional cluster states with interchangeable degrees of connections. The second set of patents address these technology issues and are able to generate the entangled photons pairs on chip as well. This is the next and necessary step towards periodic n-dimensional cluster state generation.

Theory/experimental requirements of imperfect two-qubit linear optical photonic gates

We have shown the theoretical basis and interest for this experiment. At this time it is the only apparent means of experimentally confirming the numerical data presented above, which quantifies the trade-off between fidelity and success, for the CZ or CNOT gate. The experimental setup may naturally be extended to explore the behavior of other quantum gates of interest. The components needed for the execution of the experiment are well within the means of many experimental groups. The main stumbling block is the expense of purchasing number-resolving detectors. However, any group already possessing these detectors should be able to implement this scheme with relative ease.

Nonlocality, entanglement witnesses and supra-correlations

In this area of research we have examined the structure of supra-correlations that are stronger than quantum and hence not realizable by a physical (positive) quantum state $\rho \geq 0$. The supra-correlations are intriguing because they arise from valid probability distributions, first put forth by Popescu and Rohrlich (PR), that satisfy the no-signaling principle of special relativity as well as all the usual normalization condition on the joint and marginal distributions. Thus, the fact that nature is not able to realize these supra-correlations points to hidden structure underlying how quantum correlations can be distributed amongst spacelike separated parties. Our work has examined the structure and distribution of PR correlations in 2- and 3-qubit systems by explicitly constructing “states” (not necessarily positive quantum states) that exhibit supra-correlations for a fixed, but arbitrary number, of measurements available to each party. We have shown that the PR correlations involve only solely n -party correlations amongst the n observers. We have extended this study to include n -party correlations that capture the essential features of the PR correlations and do not rely on predetermined measurements between the n participants. Additionally, by constructing constraints based on the positivity and purity of an arbitrary n -qubit state we have shown the “unreasonableness” of the PR correlations in that they encode more correlations than are physically allowed by nature [see details in Alsing12]. In future work we will couple this approach of studying how correlations are distributed amongst the n parties to the study of quantum entanglement. The study of entanglement [Horodecki09] is an important, but difficult field, only well understood for the case of two qubits (both pure and mixed), and to a lesser degree, for pure 3-qubit systems. A fruitful area to investigate next are pure 3-qubit systems, where a generalized (though non-unique) Schmidt decomposition holds [Acin00]. We purport that an examination of the distribution of correlations, bounded by physically imposed constraints on e.g. positivity and purity, coupled with the description of entanglement in terms of the tangle, as initiated in this work, can shed further light on the classification of pure tripartite systems.

Efficient cluster state generation (theory)

In this area of the research we have shown numerically [Uskov13a], that linear cluster states can be made $(9/4)=2.25\times$ more efficiently than by conventional quantum state projection methods. We have also made considerable progress [Uskov13b] in our analytic understanding of how this increase in success probability for linear cluster state generation arises. The essential idea is that to append additional qubits to a linear cluster state in order to make a larger linear cluster state, $|\psi_{in}\rangle = |C_n\rangle|+\rangle_{n+1}\cdots|+\rangle_{n+m}\cdots \rightarrow |C_{n+m}\rangle = |\psi_{out}\rangle$. the initial qubits are in well-defined *a priori* state, namely $|+\rangle_{n+1}\cdots|+\rangle_{n+m}$ where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Thus, the desired transformation (possibly non-unitary) is only required to take the particular state $|C_n\rangle|+\rangle_{n+1}\cdots|+\rangle_{n+m}$ to $|C_{n+m}\rangle$. A unitary transformation would have additionally map all the other $2^m - 1$ states orthogonal to $|C_n\rangle|+\rangle_{n+1}\cdots|+\rangle_{n+m}$ to $2^m - 1$ respective states that are orthogonal to $|C_{n+m}\rangle$ and to each other. Not requiring this additional burden is the essential reason for the speedup that we have found. For the case discussed here of $|\psi_{in}\rangle = |C_n\rangle|+\rangle_{n+1} \rightarrow |C_{n+1}\rangle = |\psi_{out}\rangle$ one sees that in (47) that only half the number conditions that would require the transformation to be unitary are necessary. Though the resulting transformation need not necessarily be unitary, we have found analytically [Uskov13b] unitary instantiations of a transformation that gives a success probability of $1/4$ (vs the conventional $1/9$). Ongoing and future research will explore experimental realization of linear cluster state generation with

success probability of $\frac{1}{4}$ and expand of the theory from linear to two dimension (grid) cluster state generation.

6.0 REFERENCES

- [Acin00] A. Acin, A. Andrianov, L. Costa, E. Jane, J.I. Latorre and R. Tarrach, “Generalized Schmidt decomposition and classification of three-quantum-bit states,” *Phys. Rev. Lett.* **85**, 1560 (2000).
- [Acin10] A. Acin, R. Augsiak, D. Cavalcanti, C. Hadley, J.K. Korbicz, M. Lewenstein, L. Masanes and M. Piani, “Unified framework for correlations in terms of local quantum observables,” *Phys. Rev. Lett.* **104**, 140404, (2010); arxiv:0911.3606.
- [Aliferis06] P. Aliferis, D. Gottesman, J. Preskill, “Quantum accuracy threshold for concatenated distance-3 codes,” *Q. Info & Comp.* **6**, 97 (2006).
- [Alsing12] P.M. Alsing and J.R. McDonald, “Nonlocality, Entanglement Witnesses and Supra-correlations,” *Proc. of SPIE* **8400**, 84000Y (2012).
- [Anderson04] E. H. Anderson, D. Ha, J. A. Liddle, “Sub-pixel alignment for direct write electron beam lithography,” *Microelectronic Eng.* **73-74**, 74-79 (2004).
- [Barnum10] H. Barnum, S. Beigi, S. Boixo, M.B. Elliot and S. Wehner., “Local quantum measurement and no-signaling imply quantum correlations,” *Phys. Rev. Lett.* **104**, 140401 (2010); arxiv:0910.3952.
- [Bell64] J.S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics* **1**, 195 (1964).
- [Bitton01] G.Bitton, *et al.*, “Novel Cascaded Ultra Bright Pulsed Source of Polarization Entangled Photons”, arXiv:quant-ph/0106122v1, (2001).
- [Branning11] D. Branning *et al.*, “Note: Scalable multiphoton coincidence-counting electronics”, *Review of Scientific Instruments* **82**, 016102, (2011).
- [Ceccarelli09] R. Ceccarelli, *et al.*, “Experimental Entanglement and Nonlocality of a Two-Photon Six-Qubit Cluster State”, *Phys. Rev. Lett.* **103**, 160401 (2009).
- [Clauser69] J.F. Clauser, “Proposed experimental tests to local hidden-variable theories,” *Phys. Rev. Lett.* **23**, 880 (1969).
- [Clem11] J. R. Clem and K. K. Berggen “Geometry-dependent critical currents in superconducting nanocircuits,” arXiv:1109.4881v1 (2009).
- [Dauler08] E. A. Dauler et al., “Photon-number-resolution with sub-30-ps timing using multi-element superconducting nanowire single photon detectors,” *Journal of Modern Optics* **56**, pp. 364-373 (2008).

- [DiVincenzo00] D.P. DiVincenzo, “The physical implementation of quantum computation,” *Fortschr. Phys.* **48**, 771 (2000).
- [Dragoman01] D. Dragoman, “Proposal for a three-qubit teleportation experiment”, *Phys. Lett. A* **288**, 121-124 (2001).
- [Drever83] Drever R. W. et al. “Laser phase and frequency stabilization using an optical resonator,” *Appl. Phys. B* **31**, 97-105 (1983).
- [Fanto10] M.L. Fanto *et al.*, “Compensated crystal assemblies for type-II entangled photon generation in quantum cluster states”, *SPIE Vol.* **7702**, 77020H (2010).
- [Fanto11] M.L. Fanto *et al.*, “Multipli-entangled photons from a spontaneous parametric down-conversion source”, *SPIE* **8057**, 805705 (2011).
- [Grover97] Grover, L.K., “Quantum mechanics helps in searching for a needle in a haystack,” *Phys. Rev. Lett.* **79**(2), 325-328 (1997).
- [Guhne09] O. Guhne and G. Toth, “Entanglement detection,” *Phys. Reports* **474**, 1-75 (2009).
- [Gurevich87] A.V. Gurevich and R.G. Mint, “Self-heating in normal metals and superconductors,” *Rev. Mod. Phys.* **59**, 941 (1987).
- [Hadfield09] R. H. Hadfield “Single-photon detectors for optical quantum information applications,” *Nat. Photonics* **3**, 696 (2009).
- [Hoffmann02] H.F. Hofmann and S. Takeuchi, “Quantum phase gate for photonic qubits using only beam splitters and postselection,” *Phys. Rev. A* **66**, 024308 (2002).
- [Horodecki09] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, “Quantum entanglement,” *Rev. Mod. Phys.* **81**, 865-942 (2009); arxiv:quant-ph/0702225.
- [Kerman07] A. J. Kerman et al. , “Constriction-limited detection efficiency of superconducting nanowire single-photon detectors,” *Appl. Phys. Lett.* **90**, 101110 (2007).
- [Kieling12] K. Kieling, J. L. O'Brien and J. Eisert, “On photonic controlled phase gates,” *New J. Phys.* **12**, 013003 (2012).
- [Knill01] E. Knill E., R. Laflamme and G.J. Milburn, “A scheme for efficient quantum computation with linear optics,” *Nature* **409**, 46 (2001).
- [Kiesel05a] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, “Linear Optics Controlled-Phase Gate Made Simple,” *Phys. Rev. Lett.* **95**, 210505 (2005).
- [Kiesel05b] N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin and H. Weinfurter, “Experimental Analysis of a Four-Qubit Photon Cluster State,” *Phys. Rev. Lett.* **95**, 210502 (2005).

- [Knill02] E. Knill, “Quantum gates using linear optics and postselection,” *Phys. Rev. A* **66**, 052306 (2002).
- [Kok07] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Linear Optical Quantum Computing with Photonic Qubits*, *Rev. Mod. Phys.* **79**, 135 (2007).
- [Kraus83] Kraus K. “Lecture Notes: States, Effects and Operations: Fundamental Notions of Quantum Theory” (Springer, New York, 1983).
- [Kwiat95] P.G Kwiat *et al.*, “New High Intensity Source of Polarization-Entangled Photon Pairs”, *Phys. Rev. Lett.* **75**, 4335-4341 (1995).
- [Kwiat99] P.G Kwiat *et al.*, “Ultrabright source of polarization-entangled photons”, *Phys. Rev. A* **60**, 773-776 (1999).
- [Langford05] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O’Brien, G. J. Pryde, and A. G. White, “Demonstration of a Simple Entangling Optical Gate and Its Use in Bell-State Analysis,” *Phys. Rev Lett.* **95**, 2105504 (2005).
- [Lemr11] K. Lemr, A. Č.J. Soubusta, K. Kieling, J. Eisert, and M. Dušek, “Experimental Implementation of the Optimal Linear-Optical Controlled Phase Gate,” *Phys. Rev. Lett.* **106**, 013602 (2011).
- [Lu07] C.Y. Lu *et al.*, “Experimental entanglement of six photons in graph states”, *Nature Physics*, **3**, 91 (2007).
- [Ma10] S.Y. Ma, *et al.*, “Probabilistic quantum network coding of M-qudit states over the butterfly network”, *Opt. Comm.* **283**, 497-501 (2010).
- [Marsili11] F. Marsili *et al.*, “Single-Photon Detector based on Ultranarrow Superconducting Nanowires,” *Nano Let.* **11**, 2048-2053 (2011).
- [Masanes06] L. Masanes, A. Acin and N. Gisin, “General properties of nonsignaling theories,” *Phys. Rev. Lett.* **73**, 012112 (2006); arxiv:quant-ph/0508016.
- [Nam11] B. Baek, A. E. Lita, V. Verma and S. W. Nam, “Superconducting a- $\text{W}_x\text{Si}_{1-x}$ nanowire single-photon detector with saturated internal quantum efficiency from visible to 1850 nm,” *Appl. Phys. Lett.* **98**, 251105 (2011).
- [Nielsen05] M.A. Nielsen, “Cluster-State Quantum Computation”, arxiv 0504097v2, (2005).
- [O’Brien07] J.L. O’Brien, *et al.*, “Optical quantum computing”, *Science* **318**, 1567 (2007).
- [O’Brien09] J. L. O’Brien, A. Furusawa, J. Vuchovic, “Photonic quantum technologies,” *Nat. Photonics* **3**, 687, (2009).

- [Okamoto05] R. Okamoto, H.F. Hofmann, S. Takeuchi, and K. Sasaki, “Demonstration of an Optical Quantum Controlled-NOT Gate without Path Interference,” *Phys. Rev. Lett.* **95**, 210506 (2005).
- [Pan12] Jian-Wei Pan, Zeng-Bing Chen, Chao-Yang Lu, H. Weinfurter, A. Zeilinger and M. Zukowski, “Multiphoton entanglement and interferometry,” *Rev. Mod. Phys.* **84**, 777 (2012).
- [Pawlowski09] M. Pawłowski, T. Paterek, D. Kaszilkowski, V. Scarani, A. Winter and M. Zukowski, “Information causality as a physical principle,” *Nature Letters* **461**, 1101 (2009).
- [Peters12] C.J. Peters *et al.*, “A Multipli-entangled Photon Source for Cluster State Generation,” *SPIE* **8400**, 84000Z (2012).
- [Popescu94] S. Popescu and D. Rohrlich, “Quantum nonlocality as an axiom,” *Found. Phys.* **24**, 379 (1994).
- [Porteous95] I.R. Porteous, “Clifford algebras and the classical groups,” Cambridge: Cambridge University Press (1995).
- [Prevedel07] R. Prevedel, *et al.*, “Experimental realization of a quantum game on a one-way quantum computer”, *New J. Phys.* **9**, (2007).
- [Ralph02] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, “Linear optical controlled-NOT gate in the coincidence basis,” *Phys. Rev. A* **65**, 062324 (2002).
- [Rangarajan09] R. Rangarajan, *et al.*, “Optimizing type-I polarization-entangled photons”, *Optics Express* **17**, 18920 (2009).
- [Raussendorf01] R. Raussendorf and H.J. Briegel, “A one-way quantum computer,” *Phys. Rev. Lett.* **86**, 5188 (2001); *ibid* “Computational model underlying the one-way quantum computer,” *Q. Info. & Comp.* **2**, 443 (2002); *ibid*, “Persistent entanglement in arrays of interacting particles,” *Phys. Rev. Lett.* **85**, 910–913, (2001); R. Raussendorf, D.E. Browne and H.J. Briegel, “Measurement-based quantum computation using cluster states,” *Phys. Rev. Lett.* **68**, 022312 (2003).
- [Reck94] Reck M., Zeilinger A., Bernstein H. J., and Bertani P. “Experimental realization of any discrete unitary operator”. *Phys. Rev. Lett.* **73**, 58-61 (1994).
- [Schumacher91] B.W. Schumacher, “Information and quantum nonseparability,” *Phys. Rev. A* **44**, 7047 (1991).
- [Schmid07] C. Schmid, *et al.*, “The entanglement of the four-photon cluster state”, *New Journal of Physics* **9**, 236-246 (2007).
- [Soeda10] A. Soeda *et al.*, “Quantum computation over the butterfly network”, *Phys. Rev. A* **84**, 012333 (2010).
- [Sohma94] S. Sohma *et al.* “Silica-based PLC Type 32x32 Optical Matrix Switch,” *Euro. Conference on Optical Communication*, 1-2 (2006).

- [Smith11] A. M. Smith, D. B. Uskov, L. H. Ying, and Kaplan L., “Imperfect linear optical photonic gates with number-resolving photodetection,” *Phys. Rev. A* **84**, 032341 (2011).
- [Svetlichny87] G. Svetlichny, “Distinguishing three-body from two-body nonseparability by a Bell-type inequality,” *Phys. Rev. D* **35**, 3006 (1987).
- [Tsirelson80] B. Tsirelson, “Quantum Generalizations of Bell's Inequality,” *Lett. Math. Phys.* **4**, 93 (1980).
- [U'ren06] A.B. U'Ren *et al.*, “Generation of two-photon states with an arbitrary degree of entanglement via nonlinear crystal super lattices”, *Phys. Rev. Lett.* **97**, 223602 (2006).
- [Uskov09] Uskov D.~B., Kaplan L., Smith A. M., Huver S. D., and Dowling J. P. “Maximal success probabilities of linear-optical quantum gates”. *Phys. Rev. A* **79**, 042326 (2009).
- [Uskov10] D. B. Uskov, A. M. Smith, and L. Kaplan, “Generic two-qubit photonic gates implemented by number-resolving photodetection,” *Phys. Rev. A* **81**, 012303 (2010).
- [Uskov13] D. B. Uskov, P.M. Alsing, M.L. Fanto, L. Kaplan and A. M. Smith, “Success rates for linear optical generation of cluster states in coincidence basis,” (submitted to *J. Phys. B*, Aug, 2013); arxiv:1306.4062.
- [Uskov14] D. B. Uskov, P.M. Alsing, M.L. Fanto, L. Kaplan and A. M. Smith, “Success rates for linear optical generation of cluster states in coincidence basis,” (in preparation for submission to *Phys. Rev. Lett.*, Jan 2014).
- [Vallone10] G. Vallone *et al.*, “Six-qubit two-photon hyperentangled cluster states: Characterization and application to quantum computation”, *Phys. Rev. A* **81**, 052301 (2010).
- [van Dam05] W. van Dam, “Implausible consequences of superstrong nonlocality,” *quant-ph/0501159* (2005).
- [VanMeter07] N. M. VanMeter, P. Lougovski, D.B. Uskov, K. Kieling, J. Eisert, and J.P. Dowling, General Linear-Optical Quantum State Generation Scheme: Applications to Maximally Path-Entangled States,” *Phys. Rev. A*, **76**, 063808 (2007).
- [Vedral97] V. Vedral, M.B. Plenio, M.A. Rippin and P.L. Knight, “Quantifying Entanglement,” *Phys. Rev. Lett.* **78**, 2275 (1997); V. Vedral, “Introduction to quantum information science”, Oxford, N.Y. (2006).
- [Walther05] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger, “Experimental one-way quantum computing,” *Nature* **434**, 169 (2005).
- [Wilde09] Wilde M.M. and Uskov D.B. “Linear-optical hyperentanglement-assisted quantum error-correcting code”. *Phys. Rev. A* **79**, 022305 (2009).

[Xiang11] Y. Xiang and W. Ren, “Bound on genuine multipartite correlations from the principle of information causality,” *Quantum Information & Computation*. **11**, 948 (2011); arxiv:1101.2971.

[Xu08] F. Xu, Z. Han, and G. Guo, “Improvements of QKD with practical photonnumber resolving detectors,” *Proc. SPIE* **7278**, 72780Y (2008).

[Yao12] Xing-Can Yao, Wang Tian-Xiong, Ping Xu, Lu He, Ge-Sheng Pan, Xiao-Hui Bao, Cheng-Zhi Peng, Lu Chao-Yang, Chen Yu-Ao, Jian-Wei Pan, *Nature Photonics* **6**, 225 (2012).

7.0 LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

2D:	2 Dimensional
3D:	3 Dimensional
α -BBO:	Alpha barium borate
AFRL:	Air Force Research laboratory
APD:	Avalanche photodiode
a-W _x Si _{1-x} :	Amorphous Tungsten Silicon
β -BBO:	Beta barium borate
BiBO:	Bismuth borate
BI:	Bell Inequality
CCD:	Charged coupled device
CCM:	Coincidence counting module
CHSH:	Clauser-Horne-Shimony-Holt
CJI:	Choi-Jamolkowski isomorphism
CNOT:	Controlled NOT (gate)
CW:	Continuous wave
CZ:	Controlled Z (gate)
fs:	femtosecond
FWM:	Four wave mixing
GVM:	Group velocity matching
HP:	High power
IW:	Integrated Waveguides
JAG:	Judge Advocate General
LiNbO ₃ :	Lithium Niobate
LS:	Least squares
MBQC:	Measurement based quantum computing
MgO:	Magnesium Oxide

MHz:	megahertz
mm:	millimeter
NbN:	Niobium Nitride
NbTiN:	Niobium Titanium Nitride
NIST:	National Institute for Standards and Technology
nm:	nanometer
NS:	No-signaling
OPO:	Optical Parametric Oscillator
PCSG:	Probabilistic Cluster State Generator
PM:	Polarization Maintaining
PPKTP:	Potassium Titanyl Phosphate
PQNS:	Post Quantum No-signaling
PR:	Popescu-Rohrlich
QM:	Quantum Mechanics
QIS:	Quantum Information Science
QPIC:	Quantum Photonic Integrated Circuit
S.E.:	Sequential Entangler
SHG:	Second harmonic generation
Si:	Silicon
Si-APD:	Silicon avalanche photodiode
SI:	Svetlichny Inequality
SNSPD:	Superconducting Nanowire Single Photon Detector
SPCM:	Single photon counting module
SPDC:	Spontaneous parametric downconversion
SR:	Special Relativity
THG:	Third harmonic generation
TPR:	Tripartite Popescu-Rohrlich

UV: Ultraviolet